Waarom zijn jouw gegevens interessant voor cyber criminelen

Caroline Loef

Presentatie voor HCC – April/Mei 2026

Jouw gegevens en cyber criminelen

- Cybercriminelen zijn voortdurend op zoek naar informatie die waardevol is.
- Jouw gegevens kunnen gebruikt worden om geld te verdienen, direct of indirect.
- Elk stukje informatie kan worden ingezet in een aanval. Ook als je denkt dat je “niets te verbergen” hebt, blijft jouw data bruikbaar voor criminelen.
- Zowel persoonlijke als zakelijke gegevens vormen een aantrekkelijk doelwit.

Financiele waarde

- Persoonsgegevens kunnen worden verkocht op de zwarte markt.
  - Ze worden gebruikt door cybercriminelen om identiteiten op te bouwen en door te verkopen.
- Data zoals BSN, adres en geboortedatum hebben directe financiële waarde.
  - Hoe completer de set, hoe hoger de prijs.
- Gegevens worden misbruikt voor identiteitsfraude.
  - Bijvoorbeeld om leningen af te sluiten, aankopen te doen of contracten te openen op jouw naam.
- Criminelen verdienen geld aan jouw digitale identiteit.
  - Soms meerdere keren, omdat gestolen data vaak opnieuw worden doorverkocht.

Type data / account	Darkweb prijs	Welke gegevens bevat dit?
Identificatienummer (SSN/BSN-achtig)	€0,90 – €5,50	Alleen uniek identiteitsnummer (BSN, SSN), soms + naam
Complete identiteit (“Fullz”)	€18 – €92	Naam, adres, geboortedatum, telefoonnummer, e-mail, BSN/ID-gegevens
Creditcardgegevens (met CVV)	€9 – €37	Kaartnummer, verloopdatum, CVV, soms adres van kaarthouder
Creditcard met hoge limiet	€101 – €110	Kaartnummer + CVV + hoge bestedingslimiet + adres
Bankaccount-logins	€184 – €920+	Inloggegevens, soms rekeningnummer, volledige identiteit, saldo-info
Verified crypto-accounts	€110 – €1.076	Inloggegevens, KYC-documenten (ID, selfie), wallet-toegang
Hacked Gmail-account	€55 – €60	E-mail, contactenlijst, reset-toegang tot andere accounts
Hacked Facebook-account	€41 – €46	Profielgegevens, vriendenlijst, privéberichten, foto’s
Rijbewijs-scan	€64 – €152	Documentscan met naam, adres, geboortedatum, pasfoto, documentnummer
Paspoort-scan	€92	Paspoortpagina: naam, geboortedatum, nationaliteit, pasfoto, MRZ-regel
Medisch dossier	tot €460+	Volledige medische historie, verzekeringsgegevens, adres, ID-gegevens
Verified high-value social accounts	€920+	Inloggegevens, volgers, verificatiebadge, profieldata, DM’s
Streaming accounts	€1 – €18	Inloggegevens, soms gekoppelde betaalkaart of adres

Toegang tot systemen

- Inloggegevens geven directe toegang tot accounts.
  - Met gestolen gebruikersnaam en wachtwoord kunnen criminelen direct in je e-mail, cloudomgevingen, bedrijfsnetwerk en persoonlijke diensten.
- Criminelen kunnen wachtwoorden resetten van andere accounts.
  - Een gehackt e-mailaccount biedt vaak toegang tot het resetten van wachtwoorden van tientallen andere diensten.
- Gehackte accounts worden misbruikt voor nieuwe aanvallen.
  - Denk aan phishing vanuit een betrouwbaar e-mailadres, misleiding van collega's of zakelijke partners of het verspreiden van malware.
- Business Email Compromise (BEC) wordt hierdoor eenvoudig.
  - Criminelen gebruiken een overgenomen account om financiële fraude te plegen, zoals het versturen van "spoedbetalingen".
- Eén datalek kan toegang geven tot compleet nieuwe systemen.
  - Veel mensen hergebruiken wachtwoorden, waardoor één gestolen wachtwoord een domino-effect kan veroorzaken.

Overname identiteit

- **Met genoeg informatie kunnen criminelen zich voordoen als jou**
  Door informatie van sociale media, gelekte databases en openbare bronnen te combineren, kan een aanvaller je digitale identiteit reconstrueren.
- Dit stelt hen in staat om:
  - Je vrienden, familie of collega's te benaderen alsof jij het bent
  - Je account te kapen op sociale media
  - Aanvragen te doen bij bedrijven waar jij klant bent
  - Je reputatie te schaden door berichten in jouw naam te sturen
- **Gevolg: je eigen identiteit wordt een wapen tegen jou ingezet.**

Sociale manipulatie

Criminelen gebruiken persoonlijke informatie om vertrouwen te winnen.	• Ze verzamelen gegevens via datalekken, sociale media, openbare bronnen en eerdere hacks om aanvallen persoonlijk en geloofwaardig te maken.
Aanvallen worden afgestemd op jouw gewoontes en gedrag.	• Denk aan berichten die lijken op eerdere gesprekken, herkenbare onderwerpen of namen van collega's, familie of leveranciers.
Social engineering speelt in op emoties en tijdsdruk.	• Veelvoorkomende triggers: urgentie, angst, hulpvaardigheid of autoriteit ("Dit moet nu gebeuren").
Voorbeelden zijn phishing, WhatsApp-fraude, neptelefoontjes en fake IT-support.	• De aanvallen worden steeds realistischer door het gebruik van echte gegevens die over jou te vinden zijn.
Hoe meer informatie criminelen over je hebben, hoe effectiever hun aanval.	• Elk klein datapunt — van je functie tot je hobby's — helpt hen een geloofwaardige boodschap te maken.

Waarom dit jou direct raakt

- Iedereen is een doelwit — niet alleen organisaties.
  - Cybercriminelen kiezen vaak voor de makkelijkste ingang: medewerkers en burgers, niet systemen.
- Jouw gedrag bepaalt het beveiligingsniveau.
  - Sterke wachtwoorden, alertheid en veilig omgaan met informatie verkleinen de kans op succesvolle aanvallen enorm.
- Schade raakt zowel privé als eventueel werk.
  - Identiteitsfraude, financiële schade, reputatieschade en verstoring van bedrijfsprocessen kunnen allemaal vanuit één datalek ontstaan.
- Cyberaanvallen zijn steeds persoonlijker en geloofwaardiger.
  - Dankzij verzamelde data en slimme manipulatie zijn aanvallen moeilijker te herkennen.
- Bewust handelen verkleint risico's voor iedereen.
  - Door zelf goed beveiligd te zijn bescherm je ook je familie, je collega's en je organisatie.

Bedrijfsmatige risico’s

- Medewerkers zijn een toegangspoort tot bedrijfsnetwerken.
  - Cybercriminelen gebruiken persoonlijke of zakelijke gegevens van medewerkers om binnen te dringen in systemen of toegang te krijgen tot interne accounts.
- Gehackte accounts kunnen leiden tot grootschalige bedrijfsinbraken.
  - Met één gehackt account kunnen criminelen lateraal bewegen binnen het bedrijfsnetwerk, systemen verkennen en meer accounts overnemen.
- Bedrijfsinformatie is waardevol voor spionage, verkoop of afpersing.
  - Denk aan contracten, projectplannen, technische documentatie, financiële gegevens of klantdata. Deze kunnen worden verkocht, misbruikt of gebruikt als afpersingsmiddel (bijv. ransomware).
- Aanvallen via medewerkers zijn zeer effectief.
  - Aanvallers misbruiken interne communicatie (“Het lijkt op een mail van een collega”), waardoor phishing geloofwaardiger en succesvoller wordt.
- Gestolen bedrijfsdata kan leiden tot financiële én reputatieschade.
  - Naast de kosten van herstel en stilstand kan openbaar gemaakte informatie leiden tot verlies van vertrouwen bij klanten, partners en stakeholders.

Waarde bedrijfsdata

Type bedrijfsdata	Wat bevat het	Indicatieve waarde op dark web	Waarom waardevol
Bedrijfslogins (e-mail / SaaS)	Inloggegevens voor O365, Google Workspace, CRM, HR-systemen	€20 – €300 per account	Directe toegang tot interne communicatie & data
Admin- of beheeraccounts	IT-, cloud- of domeinadmin	€500 – €10.000+	Sleutel tot hele omgeving (hoog risico)
VPN-/remote-access	VPN, RDP, Citrix, Zscaler e.d.	€100 – €2.000	Biedt ongemerkte toegang tot netwerk
Initial Access (IAB)	“Eerste toegang” tot organisatie	€300 – €50.000	Wordt doorverkocht aan ransomwaregroepen
Klantendatabases (PII)	Namen, adressen, e-mail, tel.nr.	€0,10 – €2 per record	Phishing, identiteitsverrijking
Financiële data (zakelijk)	IBAN, facturen, betalingsinfo	€10 – €100 per record	CEO-fraude, incasso-misbruik
HR- en personeelsdossiers	Contracten, IDs, salarissen	€50 – €500 per persoon	Gerichte afpersing, identiteitsfraude
Interne e-mails & documenten	Mailarchieven, notulen, beleid	€100 – €5.000+ per set	Chantage, spionage, reputatieschade
Broncode / intellectueel eigendom	Software, ontwerpen, R&D	€1.000 – €100.000+	Concurrentievoordeel, sabotage
Toegangslogs & security-info	Netwerkdiagrammen, SOC-info	Zelden los geprijsd	Vergemakkelijkt vervolgaanvallen
Back-ups	Volledige systemen & data	Hoog, contextafhankelijk	Onderhandelingsmiddel bij afpersing

Hoe kun je jezelf beschermen?

Hoe kun je jezelf (maar ook je omgeving) dan het beste beschermen?

1. Sterke, unieke wachtwoorden

- Gebruik lange wachtwoorden en een wachtwoordmanager.
- Gebruik nooit betzelfde wachtwoord voor meerdere accounts.
- Eén datalek mag nooit al je accounts in gevaar brengen.

2. Multifactorauthenticatie (MFA)

- Zet MFA aan voor al je belangrijke accounts.
- Zelfs als je wachtwoord wordt gestolen, blijft je account beschermd.
- Gebruik biivoorbeeld een app of sms-code als tweede stap.

3. Wees alert op verdachte berichten

- Controleer altjjd:
- Herken je de afzender?
- Klopt de formulering en de vragg?
- Is de link of bijlage verdacht?

Neem zelf contact op met afzender bij twijfell

4. Update systemen en apparaten

- Voer regelmalig updates uit voor je besturingssysteem, software en apps.
- Updates dichten bevelligingslekken die criminelen misbruiken.

5. Deel bewust en beperkt informatie

- Deel zo min mogellik privégegevens online.
- Let op wat je op sociale media zet.
- Hoe minder criminelen over je weten, hoe lastiger je te manipuleren bent.

Samenvatting & belangrijkste inzichten

- Jouw data hebben waarde voor criminelen — altijd.
  - Of het nu gaat om persoonlijke gegevens, inloggegevens of bedrijfsinformatie: alles kan misbruikt of verkocht worden.
- Gegevens worden gebruikt voor fraude, misleiding en toegang tot systemen.
  - Criminelen combineren datapunten om aanvallen persoonlijk, geloofwaardig en effectief te maken.
- Eén enkel lek kan grote gevolgen hebben.
  - Een gestolen wachtwoord of document kan leiden tot identiteitsfraude, financiële schade of een bedrijfsinbraak.
- Social engineering blijft het meest gebruikte aanvalsmiddel.
  - Aanvallers spelen in op vertrouwen, routine en menselijk gedrag.
- Bescherming begint bij bewustzijn en gedrag.
  - Sterke wachtwoorden, MFA, updates en alertheid maken het verschil.
- Iedereen speelt een rol in informatiebeveiliging.
  - Zowel privé als binnen een organisatie ben jij een belangrijke schakel in het voorkomen van cyberincidenten.

Vragen tot zover?

Waarom de Odido hack zo ernstig is

Wat is Odido en welke diensten bieden zij aan

Telecomdiensten

Odido biedt mobiele telefonie, internet en digitale communicatie aan miljoenen klanten in diverse regio's.

Klantenservice en bereik

Odido bedient miljoenen klanten en zorgt voor betrouwbare netwerken en connectiviteit.

Data beheer

Odido beheert persoonlijke en financiële data met aandacht voor veiligheid en privacy.

Odido hack februari 2026

Hoe vond de hack plaats (phishing & vishing)

Social engineering (phishing & vishing)
•Aanvallers deden zich voor als interne IT-medewerkers en misleidden Odido-medewerkers via e-mail en telefoon.

Misbruik van legitieme medewerkersaccounts
•Door verkregen inloggegevens kregen criminelen toegang tot een klantensysteem (Salesforce), zonder een technische kwetsbaarheid te hoeven misbruiken.

Geautomatiseerde gegevensverzameling
•Na binnenkomst werden grote hoeveelheden klantgegevens automatisch uit het systeem verzameld (scraping).

Tijdlijn van de Hack

Tijdlijn van de Odido-hack (februari 2026)

Samenvatting in één oogopslag:

7 feb	Hackers breken binnen bij Odido
8 feb	Hackers blijven actief, *Odido ontdekt de aanval*
8–9 feb	Toegang geblokkeerd, *experts ingeschäkeld*
9 feb	Datalek gemeld bij *Autorittei Persoonsgegevens*
10–11 feb	6,2 miljoen klanten getroffen
12 feb	Waarschuwingen naar klanten + media andäacht
12 feb	Oorzaak nog onbekend volgons RTL

Welke gegevens zijn gestolen

Persoonlijke identificatiegegevens

Namen en adressen kunnen zijn buitgemaakt en vormen een risico voor identiteitsdiefstal.

Contactinformatie

Telefoonnummers en e-mailadressen kunnen zijn gestolen, waardoor phishing en spam kunnen toenemen.

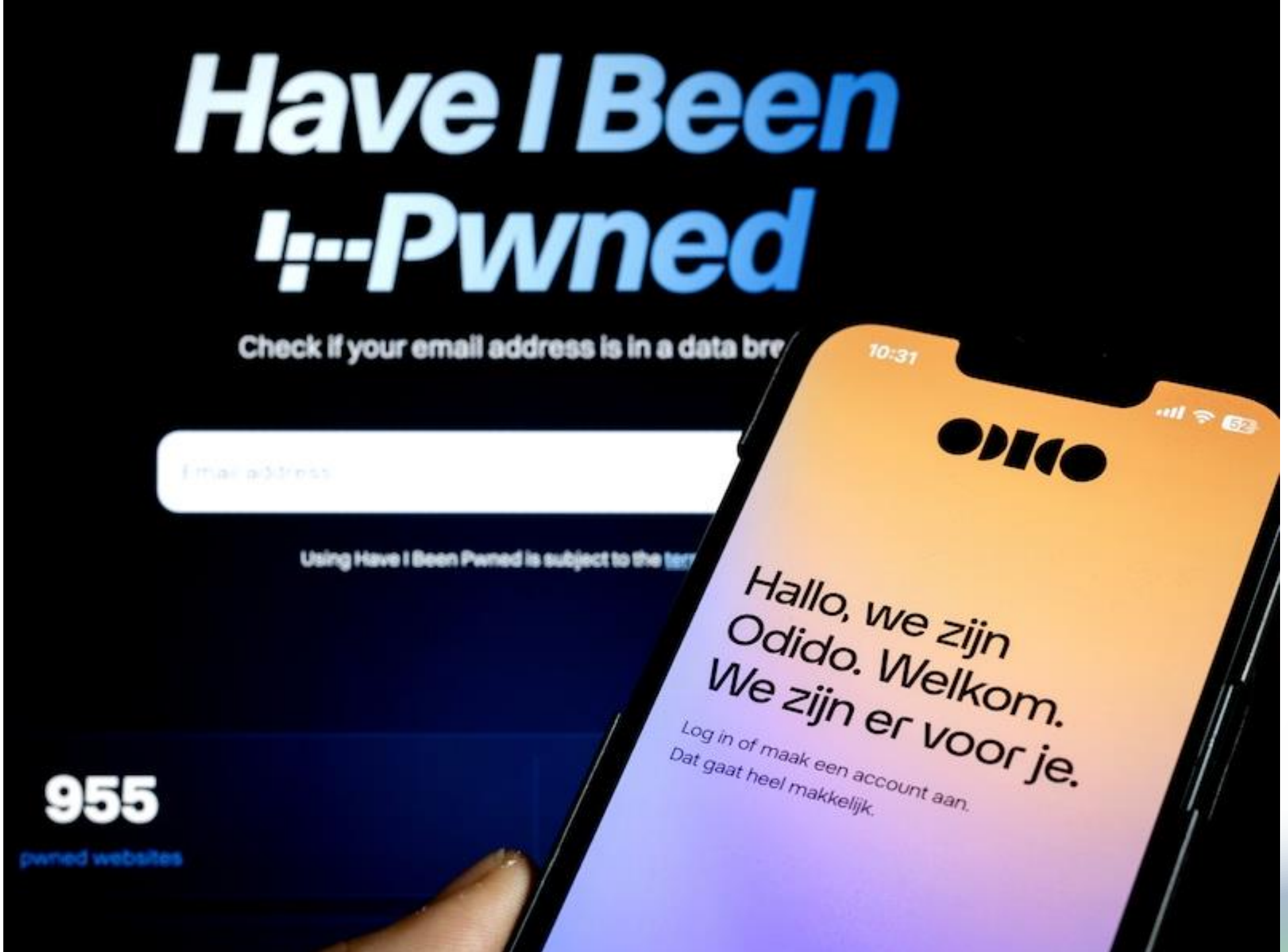
Bankgegevens

In sommige gevallen zijn ook bankgegevens buitgemaakt, wat financiële risico's met zich meebrengt.

Wachtwoorden

Wachtwoorden kunnen zijn gestolen, wat kan leiden tot onbevoegde toegang tot accounts.

Gegevenstype (zoals bij Odido)	Typische darkweb-prijs	Prijseenheid
Naam + adres (EU)	€0,20 – €1,50	per persoon
E-mailadres	€10 – €50	per 1.000
Telefoonnummer (EU)	€0,50 – €5	per stuk
Geboortedatum	Meestal niet los geprijsd	—
IBAN (zonder login)	€10 – €40	per stuk
Bankrekening mét login	€200 – €1.000+	per account
ID-documentnummer (zonder scan)	€20 – €80	per stuk
Rijbewijs-/paspoortscan (EU)	€70 – €165	per docume
“Light fullz” (naam, adres, DOB, IBAN)	€30 – €100	per persoon
Volledige fullz (incl. ID-scan)	€60 – €250+	per persoon
Interne klantnotities / contextdata	Zelden los verkocht	—


Have I Been Pwned
Check if your email address is in a data bre
Using Have I Been Pwned is subject to the ter
955
pwned websites
10:31
Hallo, we zijn Odido. Welkom. We zijn er voor je.
Log in of maak een account aan.
Dat gaat heel makkelijk.

Have I Been Pwned

Check if your email address is in a data breach

[redacted] Check

Using Have I Been Pwned is subject to the terms of use

Email Breach History

Timeline of data breaches affecting your email address

7

Data Breaches

Oh no — pwned! This email address has been found in multiple data breaches. Review the details below to see where your data was exposed.

Odido

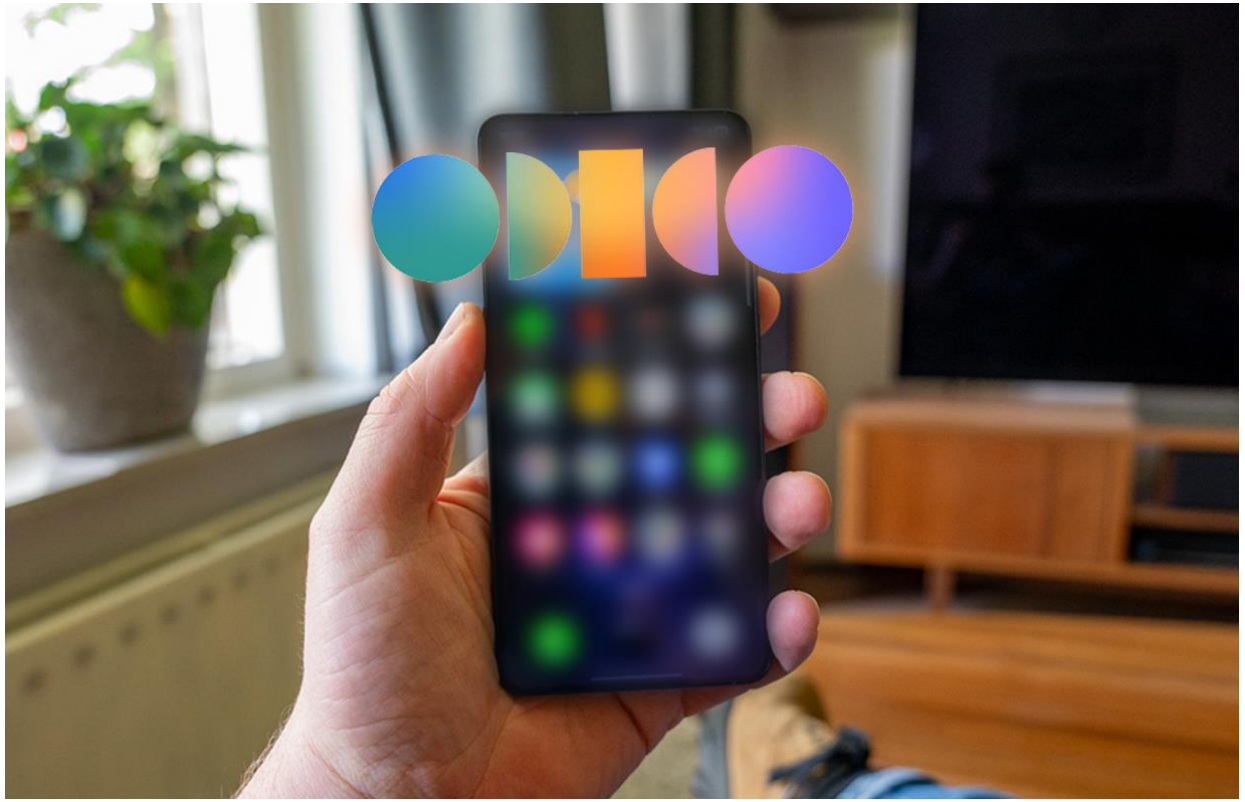
feb 2026

In February 2026, Dutch telco Odido was the victim of a data breach and subsequent extortion attempt. Shortly after, a total of 6M unique email addresses were published across four separate data releases over consecutive days. The exposed data includes names, physical addresses, phone numbers, bank account numbers, dates of birth, customer service notes and passport, driver's licence and European national ID numbers. Odido has published a disclosure notice including an FAQ to support affected customers.

Compromised data:

- Bank account numbers
- Customer service comments
- Dates of birth
- Driver's licenses
- Email addresses
- Genders
- Government issued IDs
- Names
- Passport numbers
- Phone numbers
- Physical addresses

View Details



Geachte heer/mevrouw,

Met dit bericht stellen wij u op de hoogte van een recent beveiligingsincident waarbij Odido te maken heeft gehad met ongeoorloofde toegang tot een intern systeem voor klantcontact. Als gevolg hiervan kunnen bepaalde persoonsgegevens van klanten zijn ingezien. Het betreft uitsluitend gegevens uit dit systeem; vertrouwelijke informatie zoals wachtwoorden, belhistorie en factuurgegevens zijn niet betrokken.

Wij betreuren deze situatie ten zeerste en hebben direct actie ondernomen om de toegang te blokkeren en verdere risico's te beperken. Tevens zijn gespecialiseerde externe cybersecuritydeskundigen ingeschakeld om aanvullende maatregelen te treffen en de beveiliging verder te versterken. Onze dienstverlening is niet onderbroken en blijft volledig veilig en beschikbaar voor gebruik.

Wij adviseren u om in de komende periode extra alert te zijn op mogelijke onregelmatigheden of verdachte activiteiten. Hoewel misbruik niet vanzelfsprekend is, kan dit helaas niet volledig worden uitgesloten.

In het kader van uw bescherming wijzen wij u erop dat het invullen en indienen van het compensatie-aanvraagformulier een verplichte stap is. Door dit formulier volledig en correct in te dienen, wordt vastgelegd dat u bij aantoonbare fraude aanspraak kunt maken op de geldende verzekering en eventuele financiële tegemoetkoming.

Indien u dit formulier niet (tijdig) indient, kunnen wij geen garantie bieden op enige vorm van dekking of compensatie bij een dergelijk incident. In dat geval komt het recht op vergoeding te vervallen. Wij raden u daarom nadrukkelijk aan dit proces zorgvuldig af te ronden.

De mogelijk betrokken gegevens kunnen, afhankelijk van uw situatie, bestaan uit uw naam, adresgegevens, telefoonnummer, klantnummer, e-mailadres, IBAN, geboortedatum en identificatiegegevens zoals documentnummer en geldigheidsduur.

Wij benadrukken dat de volgende gegevens geen onderdeel uitmaken van dit incident: wachtwoorden, belgegevens, locatiegegevens, factuurinformatie en kopieën van identiteitsbewijzen.

Wij achten het van groot belang om u transparant te informeren, zodat u passende voorzorgsmaatregelen kunt nemen. Uw veiligheid en privacy staan hierbij voorop. Dit incident heeft geen toegang verschaft tot locatiegegevens of persoonlijke contactinformatie.

Het voorval is gemeld bij de Autoriteit Persoonsgegevens. Daarnaast blijven wij de situatie nauwlettend volgen en u waar nodig ondersteunen. Voor aanvullende informatie en hulp hebben wij een speciale informatievoorziening ingericht.

Mocht u verdere vragen hebben, dan kunt u uiteraard contact met ons opnemen.

Hoogachtend,

CEO Odido

26 mrt 2026

Valse telefoontjes over compensatie na datalek Odido

Wij ontvangen meldingen over neptelefoontjes uit naam van Odido. In het telefoontje wordt gezegd dat het mogelijk is compensatie te krijgen vanwege het recente datalek bij Odido. Melders ontvangen vervolgens een sms met daarin een verificatiecode die moet worden voorgelezen/doorgegeven. Wat er daarna gebeurt is verschillend: sommige melders gaven aan dat er een e-sim geactiveerd was en dat ze daardoor geen toegang meer hadden tot hun simkaart. Bij andere melders kregen de oplichters op deze manier toegang tot het Odido-account, waardoor ze geen gebruik meer konden maken van hun telefoonnummer. Bij een melder werd daarnaast ook de e-mail gehackt, waarna oplichters nieuwe telefoonabonnementen afsloten en het oude nummer van de melder verwijderden.

Advies

Ontvangt u ook een dergelijk telefoontje, hang dan direct op. Odido zal u niet bellen over een compensatieregeling. Geef geen codes door die u via sms ontvangt en verwijder de sms.

Heeft u toch een code doorgegeven? Neem dan direct contact op met Odido en laat uw simkaart blokkeren. Wijzig het wachtwoord van uw account, zodat oplichters niet meer de juiste inloggegevens voor uw account hebben.

Twijfelt u over de situatie, neem dan contact met ons op, dan kunnen wij u persoonlijk advies geven.

Monitoren van je accounts en melden van verdachte activiteiten

Regelmatige controle van accounts

Controleer consistent je bankafschriften en accountactiviteiten voor ongebruikelijke transacties.

Melden van verdachte activiteiten

Meld verdachte transacties of inlogpogingen onmiddellijk bij je bank of dienstverlener om fraude te voorkomen.

- ✔️ Alert blijven op verdachte berichten
- ✔️ Bank waarschuwen en monitoren op vreemde transacties
- ✔️ Overwegen ID-kaart of rijbewijs te vernieuwen
- ✔️ 2-stapsverificatie activeren op belangrijke diensten
- ✔️ Checken of mijn gegevens ergens opduiken (bijv. via tools zoals Fobber, Opgelicht.nl-meldingen)

Vragen tot zover?

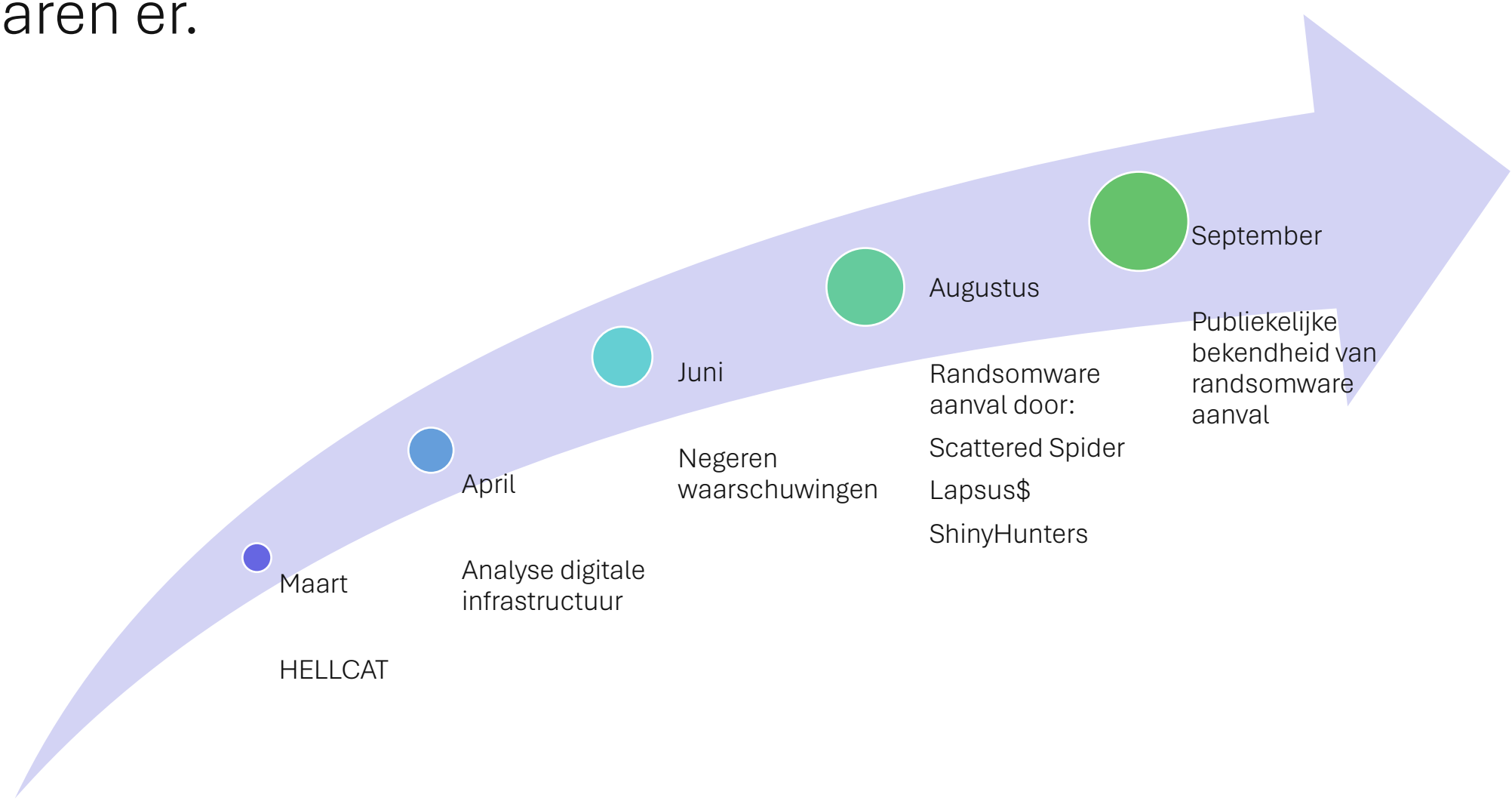
RDW

De hack bij:

Jaguar/Land Rover

2025

2025 – wat gebeurde er, wanneer, door wie en welke gevolgen waren er.



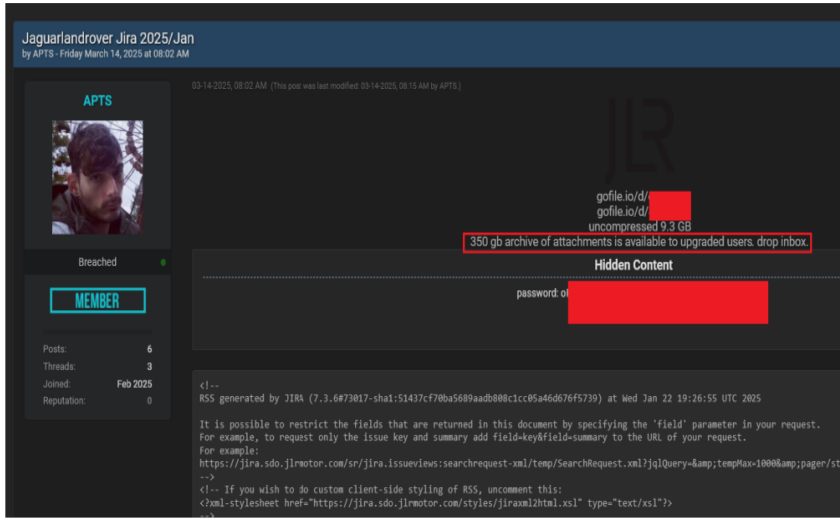
Maart 2025 – HELLCAT hack op JLR

- **Wie?** De cybercriminele groep **HELLCAT**, actief sinds 2024, richt zich op ontwikkelomgevingen en supply chains.

- **Wat?** Medewerker van **LG Electronics**, met toegang tot JLR's Jira-omgeving, kreeg via phishing of geïnfecteerde websites infostealer-malware op zijn systeem.

  Via de infostealer-malware wist HELLCAT Jira-inloggegevens van JLR-medewerkers te bemachtigen.

Hoe ? Met deze gestolen Jira-gegevens kreeg HELLCAT toegang tot JLR's interne systemen.



APTS is leaking additional data from Jaguar Land Rover

Maart 2025 - Gevolgen voor JLR

- Geen directe productie-impact

- Reputatieschade

- ±700 interne documenten en broncode gelekt

  (development logs, tracking information, source code,

  and a large employee dataset with usernames, email addresses,

  display names, and time zones)

April – Juni 2025 Waarschuwingen genegeerd

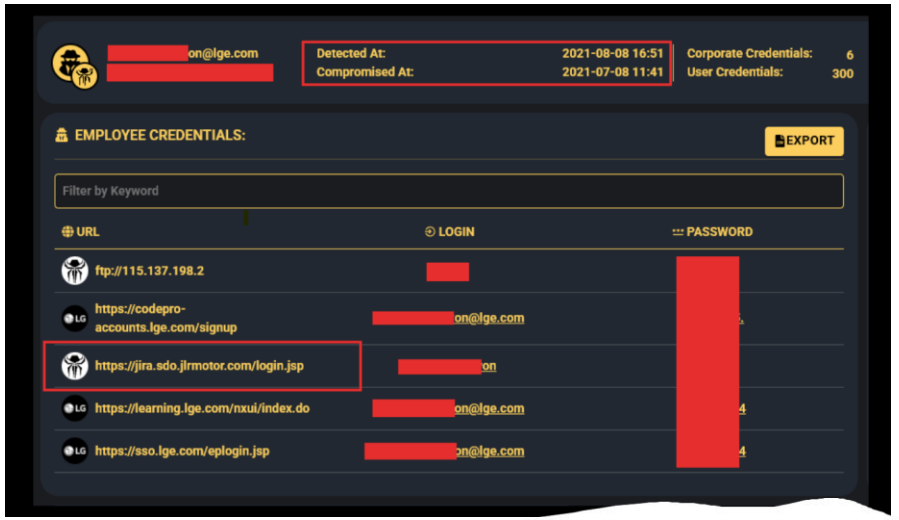
- **Wie?** Twee onafhankelijke cybersecuritybedrijven analyseerden JLR's digitale infrastructuur.

- **Hoe?** De waarschuwingen werden via officiële kanalen gemeld, maar JLR ondernam geen actie.

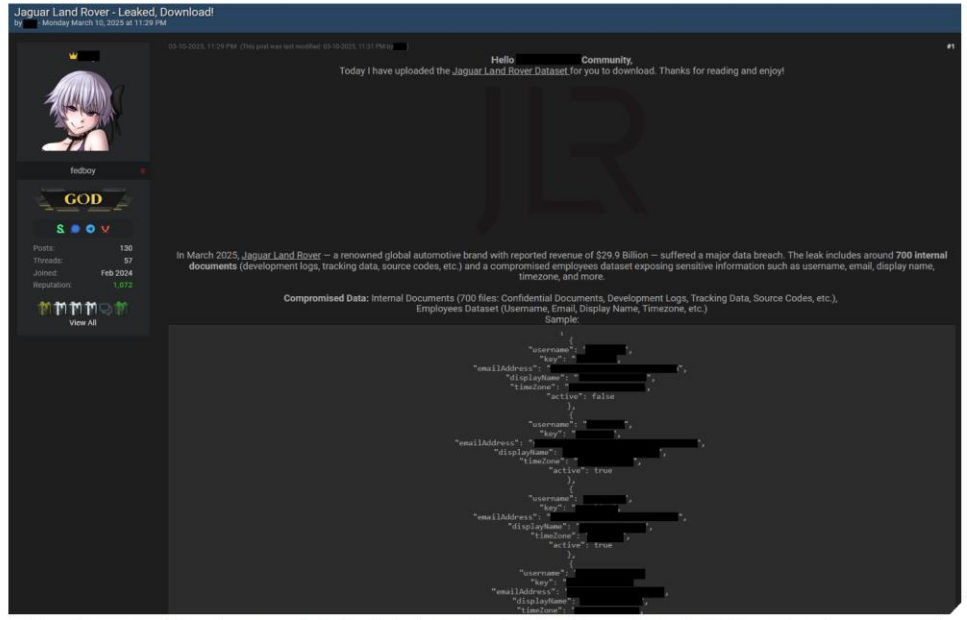
- De infrastructuur bleef kwetsbaar
- De gestolen Jira-gegevens bleven actief en bruikbaar
- De deur stond open voor een tweede, zwaardere aanval

Juli - Augustus 2025 – Samenwerkingsverband

- **Wie?**
- Samenwerking tussen **Scattered Spider**, **Lapsus$** en **ShinyHunters**, opererend onder de naam **Scattered LAPSUS$ Hunters**.



- **Waarmee?**
- Met de eerder gestolen Jira-credentials/informatie deze werden door HELLCAT verkocht aan Scattered LAPSUS$ Hunters en zo dus opnieuw gebruikt.



31 augustus 2025 – De grote aanval

Wat? De groep voerde een gecoördineerde ransomware-aanval uit op JLR’s wereldwijde IT-netwerk.

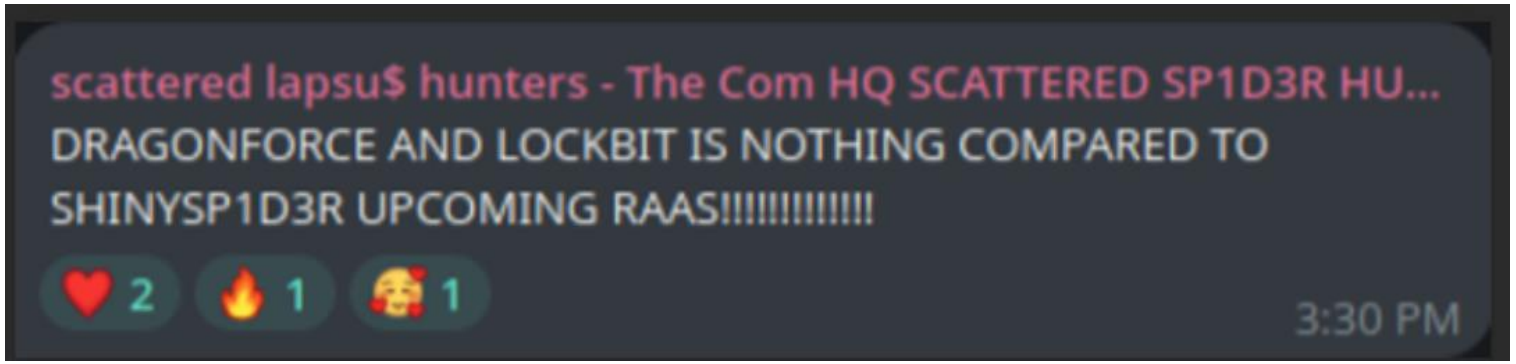
Waar? Alle productielocaties wereldwijd werden getroffen (VK (Solihull, Halewood, Wolverhampton), Slowakije, China, India, Brazilië.

Augustus – Gevolgen voor JLR

- Wereldwijde productiestop
- Tot £500 miljoen verlies per week
- Geen voertuigen konden worden geleverd/geregistreerd
- 30.000 directe werknemers en 200.000 medewerkers in de productie keten getroffen
- Reputatieschade en verlies van klantvertrouwen

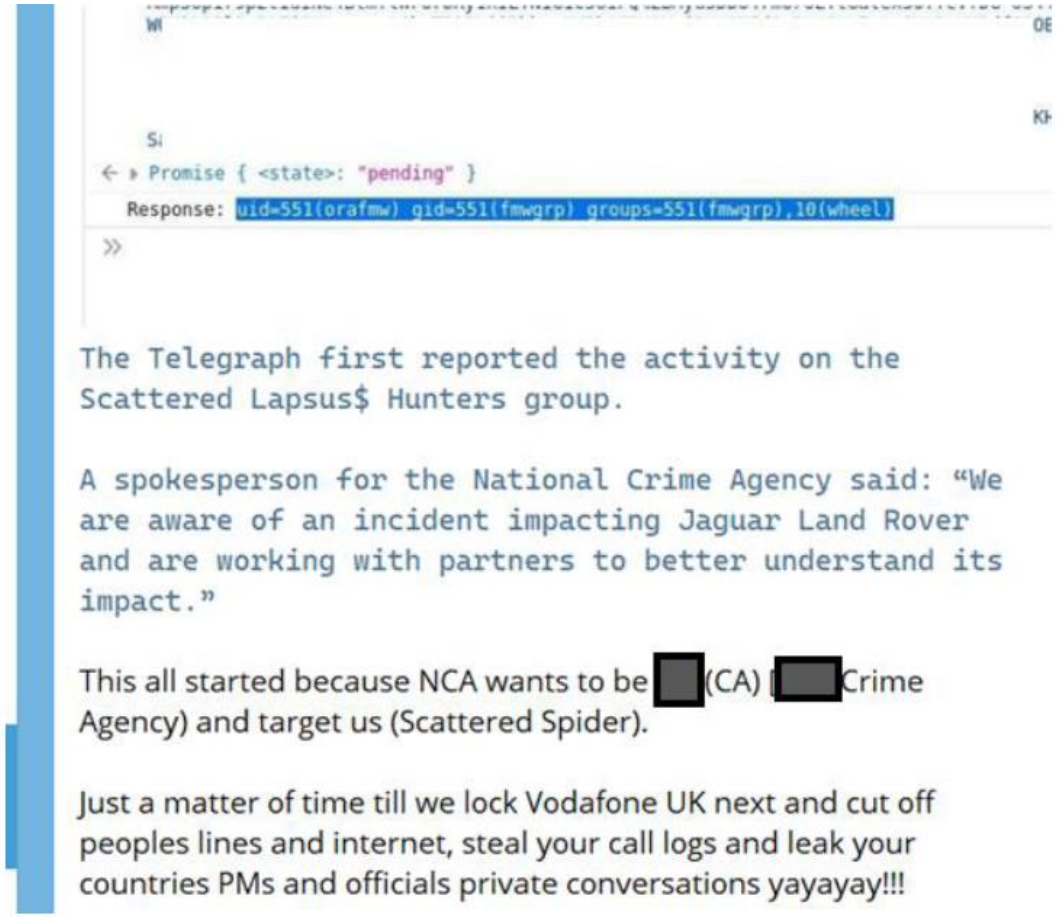
Begin September 2025 – De aanval wordt publiek

- **Wie?** De aanvallers publiceerden screenshots en data via Telegram.
- **Wat gebeurde er?** Ze richtten een kanaal op waarin ze JLR, de FBI en andere slachtoffers bespotten. Ze kondigden ook hun eigen ransomware-as-a-service aan: SH1NYSP1D3R.
- **Waar?** De communicatie vond plaats via het dark web en Telegram.
- **Hoe?**



Begin September – Gevolgen voor JLR

- Extra druk op reputatie en aandeelhouders
- Angst voor secundaire aanvallen op klanten en ketenpartners
- Versnelling van forensisch onderzoek en herstelmaatregelen



28 september: Overheidssteun

- De Britse overheid kondigde officieel aan dat zij garant zou staan voor een commerciële lening van £1,5 miljard aan JLR, bedoeld om de economische schade van de cyberaanval van eind augustus te beperken.

- De lening was specifiek bedoeld om:
- **De toeleveringsketen te ondersteunen**
  Veel kleine en middelgrote leveranciers van JLR kwamen in acute financiële problemen door de productiestop. De lening stelde JLR in staat om hen tijdig te betalen en faillissementen te voorkomen.
- **Banen te behouden**
  Met 34.000 directe werknemers in het VK en ongeveer 120.000 banen in de toeleveringsketen, was het behoud van werkgelegenheid een belangrijk motief voor de steun.
- **Herstel van productie en systemen te versnellen**
  De lening hielp JLR om IT-systemen te herstellen, productieprocessen te herstarten en de logistiek weer op gang te brengen.

Nieuws

Bank of England: Brits BBP groeit minder dan verwacht door aanval op JLR

maandag 10 november 2025, 11:46 door **Redactie**, 6 **reacties**

Het Britse bruto binnenlands product (BBP) is in het derde kwartaal met 0,2% gestegen. Dit is iets minder dan de 0,3% groei die door de Bank of England werd verwacht. De **bank** wijt de tegenvallende cijfers onder meer aan de eerdere cyberaanval op Jaguar Land Rover.

De Britse autofabrikant is in september 2025 getroffen door een cyberaanval. De aanval legde de productie van het bedrijf voor zo'n vijf weken stil. De schade bedraagt naar schatting 1,9 miljard pond, omgerekend bijna **2,2 miljard euro**. Naast Jaguar Land Rover zelf had ook de **toeleveringsketen** veel last van de productieonderbrekingen. Om de impact te beperken gaf de Britse overheid de autofabrikant eind september een lening van omgerekend zo'n **1,7 miljard euro**.

Nu blijkt dus dat de cyberaanval en daaruit voortvloeiende problemen ook de Britse economie als geheel schaden. De Bank of England schrijft de tegenvallende cijfers toe aan de cyberaanval op Jaguar Land Rover en tegenvallende export naar de Verenigde Staten (VS). De bank verwacht dat het Britse BBP in het vierde kwartaal weer herstelt tot 0,3%.

6 oktober – Herstart en herstel

- **Wie?** JLR startte gefaseerd de productie weer op, met hulp van de overheid en externe cybersecurity-experts.
- **Wat gebeurde er?** De eerste fabrieken in het VK gingen weer open. Tegelijkertijd werd een herstelplan uitgerold.
- **Waar?** Wolverhampton, Solihull en Halewood waren de eerste locaties die herstartten.
- **Hoe?** Met nieuwe segmentatie, monitoring en een vooruitbetalingsprogramma voor leveranciers.

- **Gevolgen voor JLR:**
- Langzaam herstel van productiecapaciteit
- Structurele herziening van cybersecuritybeleid
- Start van bug bounty-programma's en NIS2-compliance-traject

Stappen in de aanval JLR

Gebaseerd op de screenshots, gelekte backend code, debug logs en interne host/DNS toegang – alles gedeeld door de ShinyHunters – maakt dat je een aanvalskaart kunt maken.

Tactic	Technique ID	Technique
Initial Access	T1566	Phishing (Spear phishing to obtain credentials for internal systems)
Initial Access	T1078	Valid Accounts (using stolen Jira/employee credentials)
Execution	T1059.001	Command and Scripting Interpreter: PowerShell (if scripts were used to deploy malware in JLR systems)
Persistence	T1547.001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder (if scripts modified registry for persistence)
Privilege Escalation	T1068	Exploitation for Privilege Escalation (leveraging misconfigured host entries)
Defense Evasion	T1027	Obfuscated Files or Information (screenshots/code indicate obfuscation of activity)
Credential Access	T1555.003	Credentials from Password Stores: Credentials from Web Browsers (Jira credentials)
Discovery	T1083	File and Directory Discovery (screenshots show system paths, debug logs)
Discovery	T1046	Network Service Discovery (internal DNS and host resolution entries)
Collection	T1005	Data from Local System (debug logs, source code, backend files)
Collection	T1114	Email Collection (if internal communication/data harvested)
Exfiltration	T1041	Exfiltration over C2 Channel (sensitive code, Jira issues, debug logs)
Command and Control (C2)	T1071.001	Application Layer Protocol (C2 over HTTPS/HTTP for persistence)
Impact	T1499	Endpoint Denial of Service (threat of disruption to operational systems)
Impact	T1489	Service Stop (shutdown of IT/retail systems as part of attack strategy)

Vragen?