NB407: JOUW ODIDO DATA STAAT NU OP HET DARKWEB

Deze week werd het ergste scenario werkelijkheid: ShinyHunters publiceerde de gestolen gegevens van honderdduizenden klanten van Odido op het darkweb, inclusief IBAN nummers en paspoortnummers. We leggen uit wat criminelen nu over jou weten en welke stappen je moet nemen. Daarnaast gebruikte een Russische hacker AI om meer dan 600 FortiGate firewalls te kraken, misbruikte een hacker Claude AI voor een overheidshack en onthulde Google een Chinese spionagecampagne die bijna tien jaar lang 53 organisaties bespioneerde. CrowdStrike meldde dat AI aanvallers in recordtijd van 27 seconden door netwerken bewegen. Tot slot zoekt de politie een verdachte van bankhelpdeskfraude bij een goudsmid in Naarden. Lees alle details in de zes artikelen van deze week.

ODIDO DATA OP STRAAT, AI HACKT OVERHEDEN EN CHINESE SPIONAGE

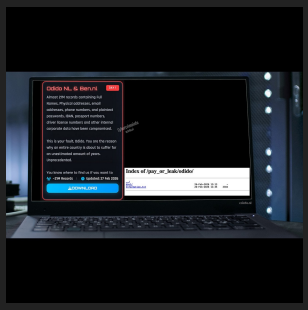
Het ultimatum van ShinyHunters is verlopen en de gestolen gegevens van honderdduizenden klanten van Odido staan nu op het darkweb, inclusief IBAN nummers en paspoortnummers. Tegelijkertijd misbruikte een hacker het AI model Claude om 150 gigabyte aan Mexicaanse overheidsdata te stelen en onthulde Google een Chinese spionagecampagne bij 53 organisaties in 42 landen. Hoeveel data is er werkelijk gelekt en wat staat er nog te wachten?

Bekijk hoeveel data er werkelijk is gelekt »

GEHACKT BIJ ODIDO: WAT CRIMINELEN NU OVER JOU WETEN

Drie lezers stuurden dezelfde vraag: wat moet ik nu doen na het datalek bij Odido? De gestolen gegevens bevatten IBAN nummers, paspoortnummers en geboortedatums, een combinatie die ethisch hacker Sijmen Ruwhof een van de ergste scenario's noemt. Weet jij al welke stappen je nu moet nemen?

Ontdek welke stappen jij nu moet nemen »



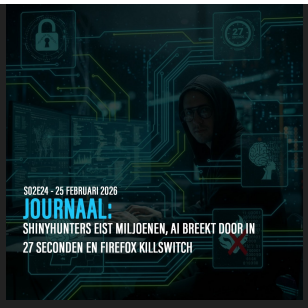
SHINYHUNTERS PUBLICEERT GESTOLEN ODIDO DATA: "DIT IS JULLIE SCHULD"

ShinyHunters heeft de eerste lading gestolen klantgegevens daadwerkelijk gepubliceerd op het darkweb met de boodschap "Dit is jullie schuld". De hackers claimen 21 miljoen records te hebben met volledige namen, adressen, IBAN nummers en zelfs wachtwoorden in leesbare tekst. De aanduiding "DAY 1" suggereert dat er meer publicaties volgen, maar hoeveel?

Lees de dreigbrief van de hackers en wat er nu op het darkweb staat »

SHINYHUNTERS EIST MILJOENEN, AI BREEKT DOOR IN 27 SECONDEN

ShinyHunters eiste miljoenen euro's losgeld van Odido en bleek ook achter datalekken bij CarGurus en Optimizely te zitten. Het CrowdStrike rapport onthulde dat aanvallers met AI nu gemiddeld in 29 minuten door een netwerk bewegen, met een record van 27 seconden. Hoe snel zouden ze bij jouw data zijn?



Zie hoe snel AI aanvallers door een netwerk bewegen »

AI KRAAKT 600 FIREWALLS, BEURZEN DALEN EN ODIDO ESCALEERT

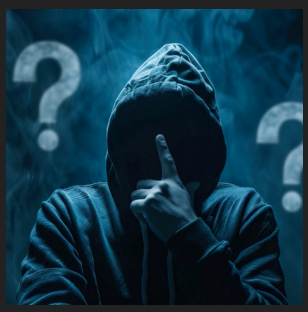
Een Russische hacker gebruikte AI om in vijf weken meer dan 600 FortiGate firewalls in 55 landen te compromitteren. De lancering van Claude Code Security stuurde een schokgolf door de cyberbeurzen en meer dan 30.000 OpenClaw instances werden gecompromitteerd. Staat jouw firewall ook op de lijst?

Bekijk hoe AI 600 firewalls kraakte in vijf weken »

GOUDSMID IN NAARDEN VOOR TONNEN OPGELICHT

Een goudsmid uit Naarden werd door oplichters misleid die zich voordeden als bankmedewerker en politieagent. Ze verloor meer dan veertig sieraden, goud en contant geld ter waarde van honderdduizenden euro's. De politie heeft camerabeelden van de verdachte, herken jij hem?

Bekijk de camerabeelden en help de politie »



CYBERCRIME QUIZ WEEK 9 - TEST JE KENNIS!

Weet jij hoeveel Odido klanten zijn getroffen door ShinyHunters? Welke cryptobeurs verloor 1,46 miljard dollar? En welk Belgisch bedrijf van de Colruyt Group verscheen op een hackerssite? Van 600 gehackte firewalls met AI tot het Sky ECC onderzoek met 1.200 veroordelingen.

Test in 20 vragen of jij alles hebt meegekregen!

Liever luisteren of kijken?

Geen tijd om te lezen? Blijf op de hoogte via uw favoriete platform. Kies voor de snelle update, de diepgaande analyse of de visuele presentatie.

Spotify Audio »
DAGELIJKS JOURNAAL (3 min)
DIEPTE ANALYSE (15 min)

YouTube Video »
VISUELE PRESENTATIE (5 min)

STRATEGISCHE DREIGINGSANALYSE VAN DIGIWEERBAAR

Dit wekelijkse rapport biedt een strategische dreigingsanalyse van actuele cyber en geopolitieke ontwikkelingen die de digitale autonomie en vitale infrastructuur van Nederland raken. Het geeft inzicht in afhankelijkheden, kwetsbaarheden en het veranderende dreigingslandschap, met focus op overheid, zorg en kritieke sectoren. Het rapport ondersteunt besluitvorming door risico's en trends helder en samenhangend te duiden.

NU 30 DAGEN GRATIS »

Help Cybercrimeinfo in de lucht te houden

Onze tools, journalen en waarschuwingen zijn gratis voor iedereen. Maar onderzoek en

hosting kosten geld. Waardeert u onze intelligence? Help ons dan met een eenmalige donatie. Elke bijdrage maakt de digitale wereld een stukje veiliger.

Ik wil graag steunen »

Bedankt voor het lezen! Deel deze nieuwsbrief gerust met vrienden, familie en collega's, samen maken we Nederland en België digitaal weerbaarder.

Tot volgende week,
Cybercrimeinfo

Share Tweet Share Pinterest Whatsapp Bluesky Mastodon