Weet jij of jouw software geraakt is door de supply chain aanvallen van deze week?

Bekijk de webversie

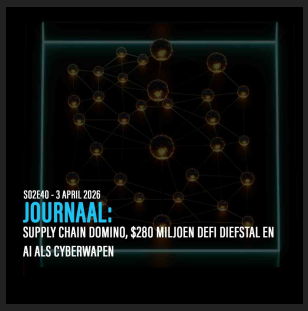
NB412: SUPPLY CHAIN ONDER VUUR, $280 MILJOEN DEFI DIEFSTAL EN AI ALS CYBERWAPEN

Deze week stond in het teken van supply chain aanvallen die steeds verder escaleren. TeamPCP vergiftigde de populaire Trivy scanner en compromitteerde de Europese Commissie via een trojaniseerd open source pakket, waarbij 350 GB aan interne data werd buitgemaakt. Noord-Koreaanse hackers infiltreerden de Axios bibliotheek met meer dan 100 miljoen wekelijkse downloads en via een Telegram sticker kon een apparaat volledig worden overgenomen. Drie Nederlandse datalekken op één dag troffen Ajax, gemeente Epe en campingplatform Eurocamp, terwijl AI nu zelfstandig kwetsbaarheden ontdekt in populaire software. De groep achter de Drift Protocol hack stal $280 miljoen aan crypto en AI maakt phishing inmiddels 450% effectiever. Dichter bij huis werd een vrouw van in de tachtig in Tilburg drie dagen lang bewerkt door oplichters die haar bankpassen stalen. Lees alle details in de vier artikelen van deze week.

DRIE NL DATALEKKEN, NOORD-KOREA HACKT AXIOS EN AI VINDT KWETSBAARHEDEN

Op één dag kwamen drie Nederlandse datalekken aan het licht bij Ajax, gemeente Epe en campingplatform Eurocamp, waarmee honderdduizenden Nederlanders werden geraakt. Noord-Koreaanse hackers wisten de populaire Axios bibliotheek met meer dan 100 miljoen wekelijkse downloads te compromitteren via social engineering van de lead maintainer. Hoe ver de schade reikt en waarom AI nu zelfstandig kwetsbaarheden vindt in software die miljoenen mensen gebruiken, lees je in het journaal.

Ontdek hoe drie datalekken Nederland troffen op één dag »



SUPPLY CHAIN DOMINO, $280 MILJOEN DEFI DIEFSTAL EN AI ALS CYBERWAPEN

AI bedrijf Mercor verloor 4 TB aan data via een supply chain aanval op het open source pakket LiteLLM en Noord-Koreaanse hackers stalen $280 miljoen van het Drift Protocol. AI maakt phishing inmiddels 450% effectiever en de Qilin ransomware groep schakelt meer dan 300 beveiligingstools uit voordat ze toeslaan. Hoe de supply chain van software zelf het grootste wapen wordt, ontdek je in dit journaal.

Lees hoe supply chain aanvallen miljoenen raken »

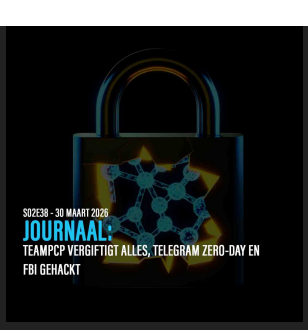
Help Cybercrimeinfo in de lucht te houden

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 »

TEAMPCP VERGIFTIGT ALLES, TELEGRAM ZERO-DAY EN FBI GEHACKT

De groep TeamPCP escaleerde hun supply chain campagne door de Trivy vulnerability scanner te vergiftigen en de Europese Commissie te hacken via een trojaniseerd pakket, waarbij 350 GB aan data werd gestolen. Via een zero day kwetsbaarheid in Telegram kon een kwaadaardige sticker een apparaat volledig overnemen en de hacktivistengroep



Handala compromitteerde het persoonlijke e-mailaccount van de directeur van de FBI. Welke andere beveiligingstools zijn geraakt en wat betekent dit voor de hele open source keten?

Bekijk hoe TeamPCP de hele supply chain vergiftigde »

GEZOCHT: PINNERS NA BANKHELPDESKFRAUDE IN TILBURG

Een vrouw van in de tachtig uit Tilburg werd drie dagen lang benaderd door oplichters via e-mail, telefoon en aan de deur. Haar bankpassen en pincodes werden gestolen en er werd gepind in Tilburg en Amsterdam. Herken jij een van de twee verdachten? Bekijk de beelden en help de politie.

Bekijk de beelden en help de politie »

CYBERCRIME QUIZ WEEK 14 - TEST JE KENNIS!

Weet jij hoeveel downloads de gehackte Axios bibliotheek per week heeft? Welk AI bedrijf verloor 4 terabyte aan data? En hoeveel procent effectiever maakt AI phishing inmiddels? Van supply chain aanvallen tot een $280 miljoen crypto diefstal.

Test in 20 vragen of jij alles hebt meegekregen!

CYBER DREIGINGSRADAR NEDERLAND & BELGIE

De Cyber Dreigingsradar van Digiweerbaar en Cybercrimeinfo is live. Als trouwe lezer van het Cyber Journaal krijg je als eerste toegang tot dit actuele dashboard dat het dreigingslandschap in Nederland en Belgie in kaart brengt.

Bekijk het actuele dreigingsniveau, ransomware activiteit, kwetsbaarheden en sectoranalyse, allemaal op basis van data die 24 uur per dag wordt verzameld uit meer dan 100 bronnen.

► BEKIJK DE CYBER DREIGINSRADAR

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)

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