Weet jij of jouw ziekenhuis getroffen is door de ChipSoft ransomware?

Bekijk de webversie

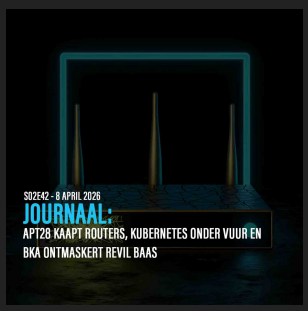
NB413: CHIPSOFT RANSOMWARE TREFT ZIEKENHUIZEN, REVIL BAAS ONTMASKERD EN TWEE FORTINET ZERODAYS

Deze week werd Nederland opgeschrikt door een ransomware aanval op ChipSoft, de grootste leverancier van patiëntendossiers in Nederland. Elf ziekenhuizen haalden uit voorzorg hun portalen offline en de Autoriteit Persoonsgegevens ontving 23 meldingen. Ondertussen onthulde de Duitse BKA de identiteit van de beruchte REvil ransomware leider UNKN, ontmantelden de FBI en het VK een Russische spionagecampagne via gehackte routers en namen aanvallen op Kubernetes met 282 procent toe. Twee kritieke zerodays in FortiClient EMS werden binnen een week ontdekt en actief misbruikt en Noord-Koreaanse hackers stalen in 2025 al meer dan twee miljard dollar aan crypto. LinkedIn bleek stilletjes browserextensies van gebruikers te volgen en een bankhelpdeskfraudeur kreeg zeven jaar cel na het stelen van 900.000 euro. De politie zoekt daarnaast meer slachtoffers van verdachte Turpien. Lees alle details in de vier artikelen van deze week.

CHIPSOFT RANSOMWARE LEGT ZORG PLAT, VENOM STEELT EXECUTIVE LOGINS EN 7 JAAR CEL

Ransomware trof ChipSoft, de grootste leverancier van patiëntendossiers in Nederland. Elf ziekenhuizen haalden uit voorzorg hun portalen offline en de Autoriteit Persoonsgegevens ontving 23 meldingen van datalekken. Hoe criminelen via het VENOM platform tegelijk topmanagers aanvallen en waarom een bankhelpdeskfraudeur zeven jaar cel kreeg, lees je in het journaal.

Lees hoe ransomware elf ziekenhuizen offline dwong »



APT28 KAAPT ROUTERS, KUBERNETES ONDER VUUR EN BKA ONTMASKERT REVIL BAAS

De FBI en het VK ontmantelden een Russische campagne waarbij de hackgroep APT28 via gehackte routers spioneerde en aanvallen op Kubernetes namen met 282 procent toe. De Duitse BKA onthulde de identiteit van de beruchte REvil ransomware leider UNKN, waarmee een van de meest gezochte cybercriminelen een gezicht kreeg. Welke andere landen en sectoren getroffen werden en wat dit betekent voor de verdediging, ontdek je in dit journaal.

Ontdek wie achter REvil schuilging »

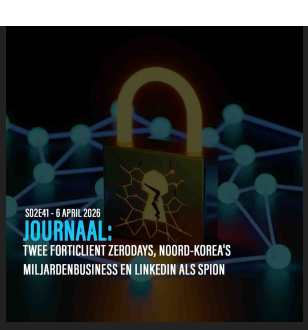
Help Cybercrimeinfo in de lucht te houden

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 »

TWEE FORTICLIENT ZERODAYS, NOORD-KOREA'S MILJARDENBUSINESS EN LINKEDIN ALS SPION

Twee kritieke zerodays in FortiClient EMS werden binnen een week ontdekt en actief misbruikt, terwijl Noord-Koreaanse hackers in 2025 al meer dan twee miljard dollar aan crypto stalen. LinkedIn bleek stilletjes duizenden browserextensies van gebruikers te volgen en het bedrijf werd aangeklaagd. Wat de FortiClient kwetsbaarheden precies mogelijk maken en hoe Noord-Korea zijn hackoperaties financiert, lees je in het



journaal.

Bekijk hoe twee zerodays Fortinet troffen »

POLITIE ZOEKT EXTRA SLACHTOFFERS VAN VERDACHTE TURPIEN

De politie is op zoek naar meer slachtoffers van verdachte Turpien, die ervan wordt verdacht meerdere mensen te hebben opgelicht via internet. Het onderzoek loopt nog en de politie vermoedt dat er meer gedupeerden zijn die zich nog niet hebben gemeld. Herken je de naam of ben je zelf slachtoffer geworden? Neem contact op met de politie.

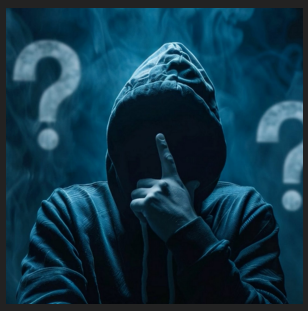
Herken jij verdachte Turpien? Bekijk de oproep »

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)



CYBERCRIME QUIZ WEEK 15 - TEST JE KENNIS!

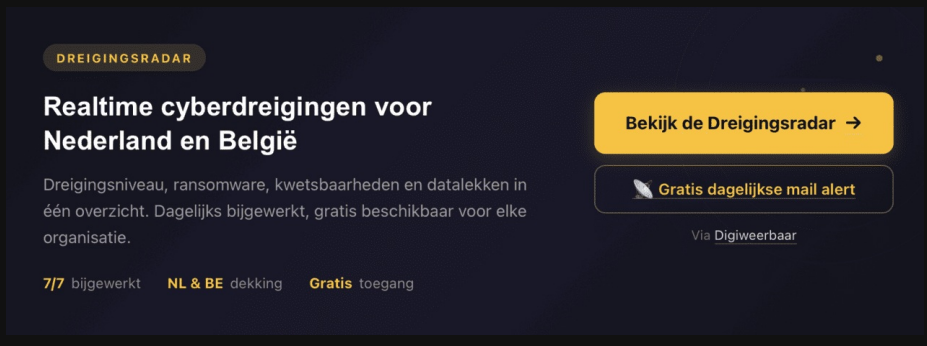
Weet jij hoeveel procent van de Nederlandse ziekenhuizen werd geraakt door de ChipSoft ransomware? Welke beruchte ransomware leider werd ontmaskerd door de Duitse politie? En hoeveel miljard dollar stalen Noord-Koreaanse hackers in 2025? Van zerodays tot Russische spionage. Test in 20 vragen of jij alles hebt meegekregen!

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.



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