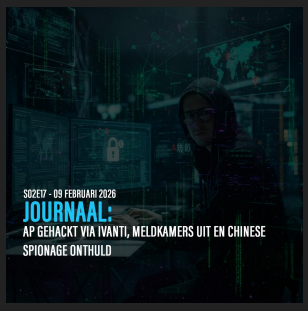
NB405: NEDERLANDSE OVERHEID GEHACKT VIA IVANTI EN ODIDO-DATALEK TREFT MILJOENEN

Deze week werd pijnlijk duidelijk hoe kwetsbaar Nederlandse overheidsinstanties zijn voor cyberaanvallen. De Autoriteit Persoonsgegevens en de Raad voor de Rechtspraak werden gehackt via twee kritieke Ivanti-kwetsbaarheden met een CVSS-score van 9.8, waarbij werknemersgegevens op straat kwamen te liggen. Telecomprovider Odido werd getroffen door een grootschalig datalek dat maar liefst 6,2 miljoen klantgegevens blootlegde, waaronder namen, adressen en zelfs bankrekeningnummers. Microsoft dichtte tijdens Patch Tuesday zes actief misbruikte zero-days en Google onthulde dat hackers uit China, Iran, Noord-Korea en Rusland AI-modellen actief inzetten als wapen voor cyberaanvallen. Daarnaast werd het updatemechanisme van de populaire teksteditor Notepad++ gecompromitteerd in een supply chain aanval. Tot slot zoekt de politie een verdachte die via een gehackt e-mailaccount identiteitsfraude pleegde in Kerkdriel. Lees alle details in de vier artikelen van deze week.

CYBER JOURNAAL

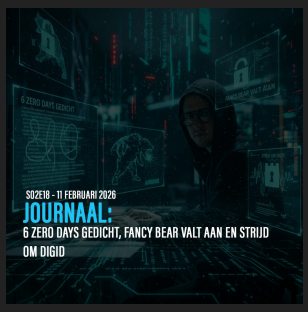


AP GEHACKT VIA IVANTI, MELDKAMERS UIT EN CHINESE SPIONAGE ONTHULD

De Autoriteit Persoonsgegevens en de Raad voor de Rechtspraak werden gehackt via twee kritieke Ivanti-kwetsbaarheden met een CVSS-score van 9.8. Werknemersgegevens zoals namen en zakelijke e-mailadressen lagen op straat. Het landelijk meldkamersysteem viel uit, waardoor politiemeldingen tijdelijk niet doorkwamen. Ondertussen onthulden onderzoekers drie Chinese spionagecampagnes, waarvan er een alleen al meer dan 70 organisaties in 37 landen compromitteerde met geavanceerde malware zoals ShadowPad en een eBPF-rootkit.

➤ LEES HET VOLLEDIGE ARTIKEL »

CYBER JOURNAAL



6 ZERO-DAYS GEDICHT, FANCY BEAR VALT AAN EN STRIJD OM DIGID

Microsoft dichtte zes actief misbruikte zero-days, waaronder een Windows Shell-lek waarbij een enkele klik op een link SmartScreen-beveiliging omzeilt. Russische spionagegroep Fancy Bear lanceerde Operation Neusploit tegen Oost-Europese overheden met malware die zich verbergt in PNG-afbeeldingen. In Nederland laaide het debat op over de mogelijke overname van cloudprovider Solvinity - die DigiD en overheidscommunicatie host - door het Amerikaanse Kyndryl.

➤ LEES HET VOLLEDIGE ARTIKEL »

CYBER JOURNAAL

ODIDO HACK TREFT MILJOENEN, AI ALS WAPEN EN SUPPLY CHAIN

Telecomprovider Odido werd getroffen door een datalek dat 6,2 miljoen klantgegevens blootlegde, waaronder namen, adressen, bankrekeningnummers en identiteitsdocumenten. Google onthulde dat hackers uit China, Iran, Noord-Korea en Rusland actief AI-modellen misbruiken voor cyberaanvallen. Daarnaast werd het updatemechanisme van Notepad++ gecompromitteerd, waarbij Chrysalis-malware werd verspreid naar gebruikers in de cloud-, energie- en overheidssector.

➤ LEES HET VOLLEDIGE ARTIKEL »

OPSPORING

IDENTITEITSFRAUDE MET GEHACKT ACCOUNT IN KERKDRIEL

Een inwoonster van Rossum ontdekte dat iemand via haar gehackte e-mailaccount kleding had besteld bij een webshop. De dader stelde slimme doorstuurregels in, waardoor bevestigingsmails automatisch in een submap verdwenen. De pakketten werden opgehaald bij pakketpunten in Kerkdriel en Rosmalen. De politie zoekt een jongeman die op camerabeelden zichtbaar is en deelt tips om jezelf te beschermen tegen deze vorm van identiteitsfraude.

➤ BEKIJK DE OPSPORINGSBEELDEN »

QUIZ

CYBERCRIME QUIZ WEEK 7 - TEST JE KENNIS!

Hoeveel klantgegevens lekte Odido? Welke overheidsinstanties werden gehackt via Ivanti? En weet jij welke landen AI inzetten voor cyberaanvallen? Deze week was vol grote incidenten - van zes Microsoft zero-days tot een arrestatie in Dordrecht voor de JokerOTP phishing tool. Test in 20 vragen of jij alles hebt meegekregen!

➤ DOE DE QUIZ »

RAPPORT

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 »

LUISTER & KIJK

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)

SUPPORT

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