NB409: RANSOMWARE RECORDJAAR EN JOUW BEHEERTOOLS ZIJN HET DOELWIT

Deze week bracht het dreigingslandschap alles in een stroomversnelling. Onderzoekers ontdekten phishing die onzichtbaar is voor beveiligingstools via misbruik van internetinfrastructuur, terwijl Huntress een stijging van 277 procent rapporteerde in het misbruik van beheertools als ScreenConnect en AnyDesk. NCC Group telde bijna achtduizend ransomware incidenten in 2025 en ShinyHunters dreigt nu 400 organisaties via misconfiguraties in Salesforce, waaronder Odido. Drie gelijktijdige aanvallen op de toeleveringsketen troffen ontwikkelaarsplatforms en de Iraanse groep Handala wiste data van meer dan 200.000 systemen bij medisch technologiebedrijf Stryker. Microsoft repareerde 83 kwetsbaarheden, waarvan een aanval via het Preview Pane zonder enige klik. Tot slot startte de politie "Game Over?!" en toont camerabeelden van 100 verdachten van bankhelpdeskfraude. Lees alle details in de vier artikelen van deze week.

PHISHING WORDT ONZICHTBAAR, BEHEERTOOLS WORDEN WAPENS

Onderzoekers ontdekten een phishingtechniek die het .arpa domein misbruikt om volledig onzichtbaar te worden voor beveiligingstools. Tegelijk rapporteert Huntress een stijging van 277 procent in het misbruik van beheertools als ScreenConnect en AnyDesk, terwijl drie grote datalekken miljoenen mensen raken. Hoe aanvallers de fundamenten van het internet omvormen tot een aanvalswapen, lees je in het journaal.

Ontdek hoe phishing via internetinfrastructuur onzichtbaar wordt »

RANSOMWARE OP RECORDHOOGTE EN NEDERLAND IN HET VIZIER

NCC Group registreerde bijna achtduizend ransomware incidenten in 2025, een stijging van vijftig procent ten opzichte van het jaar ervoor. ShinyHunters dreigt nu 400 organisaties via misconfiguraties in Salesforce en ook Odido en Ben staan centraal in de zaak. Hoe deepfakes en autonome AI bots het dreigingslandschap fundamenteel veranderen, ontdek je in dit journaal.

Bekijk hoe ShinyHunters 400 organisaties afperst via Salesforce »

SUPPLY CHAIN ONDER VUUR, WIPERS TREFFEN MULTINATIONALS

Drie afzonderlijke aanvallen op de toeleveringsketen troffen gelijktijdig ontwikkelaarsplatforms, terwijl de Iraanse groep Handala data wiste van meer dan 200.000 systemen bij medisch technologiebedrijf Stryker in 79 landen. Microsoft bracht de grootste Patch Tuesday van het jaar uit met 83 kwetsbaarheden, waarvan een aanval via het Preview Pane zonder enige klik. Welke van jouw softwarepakketten getrojaniseerd kunnen zijn, lees je in het journaal.

Zie welke softwarepakketten getrojaniseerd bleken »

GAME OVER: POLITIE TOONT 100 FRAUDEVERDACHTEN

De Nederlandse politie startte onder de naam "Game Over?!" een grootschalig opsporingsoffensief waarbij camerabeelden

van 100 verdachten van bankhelpdeskfraude worden getoond op digitale schermen in heel Nederland. Het aantal incidenten met nepagenten steeg in 2025 naar ruim 13.000 en de slachtoffers zijn voornamelijk kwetsbare ouderen die hun spaargeld verliezen. Herken jij een van de verdachten? Vanaf 23 maart worden de beelden ongeblurd getoond.

Bekijk de beelden en help de politie »

CYBERCRIME QUIZ WEEK 11 - TEST JE KENNIS!

Weet jij hoeveel ransomware incidenten NCC Group telde in 2025? Welke Iraanse groep wiste data bij Stryker in 79 landen? En hoeveel verdachten toont de politie in "Game Over?!"? Van onzichtbare phishing en misbruikte beheertools tot aanvallen op de toeleveringsketen. Test in 20 vragen of jij alles hebt meegekregen!

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