Cybercrimeinfo - cyberdreigingsanalyse (Openbare versie)

07-11-2025:

RTV Noord slachtoffer van hack, gevolgen voor uitzendingen en platforms

RTV Noord is het slachtoffer geworden van een cyberaanval, die aanzienlijke gevolgen heeft voor de uitzendingen en publicaties op hun verschillende platforms. De hack werd ontdekt op donderdagochtend, waardoor medewerkers tijdelijk niet meer toegang hadden tot de systemen. Ondanks de verstoring bleef de omroep in staat om uitzendingen voort te zetten, hoewel dit met tijdelijke ongemakken gebeurde. De live-uitzendingen via de website en app waren echter niet beschikbaar, en de normale berichtgeving lag stil. De omroep blijft actief op sociale media, maar in beperkte mate. Er werd een bericht achtergelaten door de hackers, maar hierover zijn geen details gedeeld. De technische ploeg wordt ondersteund door experts om het probleem op te lossen. De politie is nog niet ingeschakeld, aangezien de focus eerst ligt op het herstellen van de diensten van de omroep.

Ransomware-aanval op Amerikaanse staat begon met besmette download

Een ransomware-aanval op de Amerikaanse staat Nevada, die 28 dagen lang systemen platlegde, begon met het downloaden van een besmette systeembeheertool door een ambtenaar. De tool werd gedownload vanaf een malafide website die zich voordeed als de legitieme bron. De aanvallers hadden al enkele maanden eerder toegang verkregen tot het netwerk van de staat. Via de malware werd een backdoor geïnstalleerd, waarna de aanvallers meer systemen binnen het netwerk compromitteerden. De ransomware werd uiteindelijk uitgerold op meerdere servers, waardoor vitale diensten tijdelijk offline gingen. De staat besloot geen losgeld te betalen en betaalde minstens 1,5 miljoen dollar aan herstelkosten. Dankzij externe hulp werd het grootste deel van de data hersteld, waarna de diensten weer online kwamen. In reactie op het incident heeft de staat besloten gedecentraliseerde beveiligingsdiensten stop te zetten en te kijken naar een meer gecentraliseerde aanpak.

Sandworm-hackers gebruiken dataverwijderaars om Oekraïens graansector te verstoren

De Russische hackergroep Sandworm heeft meerdere varianten van dataverwijderende malware ingezet in aanvallen op Oekraïense organisaties in de

onderwijs-, overheids-, energie-, logistieke en graansectoren, de belangrijkste bron van inkomsten voor het land. Deze aanvallen vonden plaats in juni en september 2025 en vormen een voortzetting van de destructieve operaties van Sandworm. Het doel van de dataverwijderaars is het permanent vernietigen van gegevens, waardoor herstel vrijwel onmogelijk is. Eerder werden vergelijkbare aanvallen al uitgevoerd tegen Oekraïense infrastructuur, maar de graansector wordt nu nadrukkelijker aangevallen om de oorlogseconomie van Oekraïne te verzwakken. Sandworm blijft zijn aanvallen combineren met spionageactiviteiten, maar dataverwijderaars vormen nog steeds een kerncomponent van hun strategie tegen Oekraïense doelen.

Amerikaanse Congressional Budget Office getroffen door vermoedelijke buitenlandse cyberaanval

De Amerikaanse Congressional Budget Office (CBO) heeft bevestigd dat het slachtoffer is geworden van een cyberaanval, vermoedelijk uitgevoerd door buitenlandse hackers. De aanval leidde mogelijk tot de blootstelling van gevoelige gegevens. CBO-gemachtigde Caitlin Emma meldde dat het incident snel werd geïdentificeerd, waarna maatregelen werden genomen om de aanval te beperken. Extra beveiligingsmaatregelen en monitoring zijn ingevoerd om toekomstige aanvallen te voorkomen. Het CBO biedt wetgevers economische analyses en kostenramingen voor wetsvoorstellen. De aanval zou documenten zoals conceptrapporten en interne communicatie kunnen hebben blootgesteld. Hoewel het incident vroeg werd gedetecteerd, zijn er zorgen over de blootstelling van e-mails en communicatie tussen CBO-analisten en congresleden. Dit incident komt na eerdere aanvallen op andere Amerikaanse overheidsinstellingen, waaronder het ministerie van Financiën, waar de Chinese APT-groep Silk Typhoon van betrokken werd. Het onderzoek naar het incident is nog gaande.

TwoNet beweert websites in België te hebben aangevallen met DDoS-aanvallen

De cyberaanval van TwoNet richtte zich op meerdere websites in België. De aanvallen betroffen de gemeentelijke websites van Beveren, Berlaar en Lochristi, waarbij TwoNet beweerde verantwoordelijk te zijn voor de verstoring. DDoS-aanvallen, die de betrokken websites overbelasten met verkeer, kunnen aanzienlijke schade veroorzaken, zowel op technisch als op financieel vlak. Het is nog onduidelijk of er gegevens zijn gestolen of dat er andere vormen van schade zijn aangericht.

Dergelijke aanvallen vormen een voortdurende bedreiging voor de digitale infrastructuur van zowel overheidsinstellingen als andere organisaties. De impact van deze cyberaanvallen benadrukt het belang van robuuste beveiligingsmaatregelen en de noodzaak voor bedrijven en overheden om zich goed voor te bereiden op dergelijke dreigingen.

DDoS-aanvallen op Belgische websites door NoName

Op 6 november 2025 beweert de hacker-groep NoName meerdere websites in België te hebben aangevallen met een DDoS-aanval. De getroffen websites omvatten grote organisaties zoals ENGIE Electrabel, Elia Group, het Directoraat-Generaal voor Statistiek België, de Haven van Antwerpen-Brugge en de Brusselse Intercommunale Vervoermaatschappij. Deze aanval maakt deel uit van een breder patroon van cyberaanvallen gericht op vitale infrastructuur en overheidsinstellingen in België. NoName heeft de verantwoordelijkheid voor de aanvallen opgeëist, wat wijst op de groeiende dreiging van dergelijke cyberaanvallen in de regio. De gevolgen van de DDoS-aanvallen kunnen variëren van tijdelijke verstoringen van de diensten tot schade aan de reputatie van de getroffen organisaties.

Russisch hackerscollectief NoName maakt van cyberterreur een spel

Het Russische hackerscollectief NoName heeft een unieke manier bedacht om cyberaanvallen te stimuleren. Door online vrijwilligers te ronselen en hen te belonen op basis van hun aanvallen, wordt cyberterrorisme gepromoot als een soort wedstrijd. Het collectief houdt scoreborden bij waarop de deelnemers worden gerangschikt op het aantal succesvolle DDoS-aanvallen dat zij hebben uitgevoerd. De leider van de ranglijst, ZephyrKA, heeft maar liefst 339 miljoen aanvallen uitgevoerd. NoName heeft zijn invloed ook in België gevoeld, met verstoringen op websites van bedrijven zoals Proximus, Scarlet en UZ Gent. De tactiek van het hackerscollectief is ontworpen om mensen aan te moedigen om meer en langer aan te vallen, waarbij ze de daden van sabotage of verstoring in de vorm van een spel presenteren. Het collectief staat bekend om zijn pro-Russische standpunten en operaties in een globale context.

Kimsuky-hackers misbruiken VS Code-extensies voor ransomware-aanvallen via GitHub

Een recent rapport onthult hoe de Noord-Koreaanse hackergroep Kimsuky, actief sinds 2012, gebruik maakt van JavaScript- gebaseerde malware via VS Code-extensies om systemen binnen te dringen. De malware is ontworpen om command-and-control-infrastructuur op te zetten en wordt ingezet voor spionage en supply chain-aanvallen. De aanvallen beginnen met een eenvoudig JavaScript-bestand, genaamd Themes.js, dat wordt gebruikt als een dropper. Na initiële infectie verstuurt het bestand een verzoek naar een command-and-control-server om meer systemen te infecteren. Het malwarepakket voert gedetailleerde informatieverzameling uit over het doelapparaat, inclusief hardware- en netwerkconfiguraties. De malware is ontworpen om onopgemerkt te blijven door gebruik te maken van legitieme Windows-tools voor persistente toegang. De campagne lijkt gericht op langdurige infiltratie, wat wijst op de verfijning van de aanvallen door Kimsuky.

FSUE RADON-database gelekt

Op 4 november 2025 werd een database van FSUE RADON, een staatsbedrijf uit Rusland dat zich bezighoudt met het beheer van radioactief afval, gelekt. De database bevatte gevoelige informatie, zoals e-mailadressen, telefoonnummers, bedrijfsnamen, tester-informatie, rapportcommentaren en statistieken van tests. Ook werden interne gebruikers-ID's en gegevens over de staat van systemen onthuld. De gegevens werden gepubliceerd door een onbekende dreigingsactor, die bewijs van de inbraak deelde, inclusief een fragment van de database en een link naar het volledige SQL-bestand. FSUE RADON is verantwoordelijk voor het transport, de behandeling en de opslag van radioactief afval, en levert ook stralingsveiligheidsdiensten. Het lek heeft aanzienlijke bezorgdheid gewekt vanwege de mogelijke gevolgen voor de betrokken organisaties en hun systemen.

Cisco dicht kritiek lek in callcenter-software

Cisco heeft beveiligingsupdates uitgebracht voor een ernstige kwetsbaarheid in de Unified Contact Center Express (UCCX) software. Deze software, die wordt gebruikt door middelgrote bedrijven om callcenters te beheren, bevat twee kritieke beveiligingslekken: CVE-2025-20354 en CVE-2025-20358. Het gevaarlijkste lek, CVE-2025-20354, stelt ongeauthenticeerde aanvallers in staat om willekeurige

bestanden te uploaden en commando's met rootrechten uit te voeren op de UCCX-server. De kwetsbaarheid heeft een impactscore van 9.8. De andere kwetsbaarheid, CVE-2025-20358, maakt het mogelijk om scripts met adminrechten uit te voeren, met een impactscore van 9.4. Cisco heeft geen meldingen van actief misbruik ontvangen, maar raadt klanten aan de beveiligingsupdates zo snel mogelijk te installeren.

1,3 miljard gestolen wachtwoorden toegevoegd aan Have I Been Pwned

De datalekzoekmachine Have I Been Pwned heeft 1,3 miljard gestolen wachtwoorden en 2 miljard gecompromitteerde e-mailadressen toegevoegd aan zijn database. De nieuwe data werd verzameld uit zogenaamde credential stuffing-aanvallen, waarbij gestolen inloggegevens geautomatiseerd worden gebruikt om toegang te verkrijgen tot accounts op verschillende websites. Deze aanvallen zijn effectief wanneer gebruikers hun wachtwoorden hergebruiken en bedrijven onvoldoende bescherming bieden tegen dergelijke geautomatiseerde pogingen. De meeste gestolen e-mailadressen waren al bekend bij de zoekmachine, maar de toevoeging van de wachtwoorden bevatte een aanzienlijk aantal nieuwe gegevens. Beheerders kunnen nu via de zoekmachine controleren of de wachtwoordhashes in hun systemen overeenkomen met de gecompromitteerde gegevens. Dit geeft hen de mogelijkheid om maatregelen te nemen om de veiligheid van hun systemen te verbeteren.

ClickFix-malwareaanvallen evolueren met ondersteuning voor meerdere besturingssystemen en videohandleidingen

De ClickFix-malwareaanvallen zijn geavanceerd door toevoeging van videohandleidingen die slachtoffers door het zelfinfectieproces leiden, evenals een timer die druk uitoefent op het slachtoffer om risicovolle acties snel uit te voeren. Daarnaast detecteert de aanval automatisch het besturingssysteem van de gebruiker om de juiste commando's te leveren. Bij de meeste ClickFix-aanvallen wordt gebruikgemaakt van social engineering, waarbij slachtoffers worden misleid om schadelijke code of opdrachten uit te voeren. Nieuwere aanvallen bevatten een video die de aanvallen minder verdacht maakt. De aanvallers gebruiken bekende kwetsbaarheden in verouderde WordPress-plug-ins of SEO-technieken om hun kwaadaardige JavaScript op webpagina's te injecteren. Onder de gebruikte payloads bevinden zich onder andere PowerShell-scripts en MSHTA-executables. Er wordt

verwacht dat toekomstige ClickFix-aanvallen volledig in de browser kunnen plaatsvinden, waardoor traditionele beveiligingsmaatregelen mogelijk worden omzeild.

Malicious VS Code-extensie ontdekt met ingebouwde ransomware-functionaliteiten

Onderzoekers hebben een kwaadaardige Visual Studio Code-extensie ontdekt, genaamd "susvsex", die ransomware-functionaliteiten bevat. Deze extensie, die vermoedelijk met behulp van kunstmatige intelligentie is gemaakt, werd op 5 november 2025 geüpload door de gebruiker "suspublisher18" en bevatte een beschrijving "Just testing". De extensie maakt gebruik van een functie die bestanden in een opgegeven directory comprimeert, uploadt naar een externe server, en deze vervolgens versleutelt. Gelukkig is deze extensie momenteel beperkt tot een testdirectory, maar de functionaliteit kan eenvoudig worden aangepast. De extensie maakt gebruik van GitHub als command-and-control-server en zoekt naar nieuwe opdrachten in een privérepository. Microsoft heeft inmiddels de extensie uit de officiële VS Code-marktplaats verwijderd. Dit incident benadrukt de gevaren van open-source extensies en de noodzaak voor developers om zorgvuldig te zijn bij het installeren van packages.

Phishingcampagne 'I Paid Twice' gericht op Booking.com hotels en klanten

Een recente phishingcampagne heeft hotels wereldwijd getroffen, waarbij aanvallers e-mails verzonden vanuit gecompromitteerde Booking.com accounts van hotels. De aanvallers gebruikten malafide links die via de ClickFix-techniek malware, waaronder PureRAT, verspreidden. Deze malware stelt de aanvallers in staat om beheerdersaccounts van hotels te compromitteren en vervolgens gasten via valse e-mails en WhatsApp-berichten opnieuw te laten betalen voor hun reserveringen, wat resulteert in financiële schade. De malware werd geleverd door PowerShell-opdrachten, die systematische gegevensverzameling en verdere infectie van het systeem mogelijk maakten. De aanvallers verkochten ook gestolen inloggegevens van Booking.com in ondergrondse marktplaatsen. Dit frauduleuze model wordt breed gedistribueerd via cybercriminaliteitsforums, wat het voor criminelen gemakkelijker maakt om deze tactieken op grote schaal toe te passen.

Risico's van mobiele, IoT- en OT-systemen voor de publieke sector

De afhankelijkheid van verbonden technologieën in de publieke sector brengt steeds meer risico's met zich mee. Zscaler's ThreatLabz-rapport 2025 benadrukt de opkomst van bedreigingen door kwetsbaarheden in mobiele apparaten, IoT-systemen en legacy OT-omgevingen. Afgelopen jaar was er een stijging van 370% in IoT-aanvallen op overheidsystemen, evenals een toename van 147% in mobiele dreigingen. Vooral in de gezondheidszorg werden mobiele aanvallen met 224% toegenomen, met name gericht op Android-malware. Scholen en universiteiten ervaren ook een sterke stijging in IoT-aanvallen, met een 861% toename in het afgelopen jaar. Deze dreigingen hebben grote gevolgen voor publieke diensten, waarbij kwetsbare apparaten en systemen het risico op verstoringen vergroten. Zscaler beveelt aan om een zero trust-architectuur te implementeren om de risico's te beheersen en mobiele en IoT/OT-systemen in de publieke sector beter te beveiligen.

Cybersecurity forecast 2026 – Google waarschuwt voor AI-verbeterde dreigingen

In het jaarlijkse cybersecurity-rapport van Google Cloud wordt een dreigende toekomst geschetst voor 2026. Bedreigers passen geavanceerde technologieën, waaronder kunstmatige intelligentie (AI), steeds vaker toe als fundamentele tools in hun aanvallen. Dit markeert een verschuiving van experimentele naar operationele toepassingen van deze technologieën. In 2026 zullen zowel aanvallers als verdedigers zich snel aanpassen aan nieuwe technologieën, waarbij AI steeds vaker wordt ingezet voor snellere en effectievere aanvallen. Specifieke dreigingen, zoals het manipuleren van AI-systemen en het gebruik van stemkloning voor social engineering, worden steeds gebruikelijker. Ook virtualisatielaag-kwetsbaarheden worden een belangrijke zorg, waarbij succesvolle aanvallen volledige controle over digitale infrastructuren kunnen opleveren. Naast cybercriminaliteit nemen ook geopolitieke cyberactiviteiten van landen zoals China, Rusland en Noord-Korea toe, wat de complexiteit van de dreigingslandschap vergroot.

Kimsuky groep zet EndClient RAT in om gebruikers aan te vallen via gestolen code-signing certificaten

De EndClient RAT, een geavanceerde Remote Access Trojan, is opgedoken als een ernstige dreiging die gericht is op mensenrechtenactivisten uit Noord-Korea. De

malware, toegeschreven aan de Kimsuky groep, maakt gebruik van gestolen code-signing certificaten om antivirusbescherming te omzeilen en Windows SmartScreen waarschuwingen te ontwijken. De aanval wordt gekarakteriseerd door sociale engineering en het gebruik van legitiem uitziende installatiepakketten, zoals een MSI-bestand genaamd "StressClear.msi", dat een module voor Zuid-Koreaanse bankauthenticatie bevat. Na installatie zorgt de malware voor persistente toegang via geavanceerde technieken, zoals het instellen van geplande taken en polymorfe variaties om detectie te vermijden. Deze aanval heeft minstens 40 bevestigde slachtoffers, voornamelijk binnen de mensenrechtencommunity, maar de volledige omvang blijft onduidelijk door het lage aantal antivirusdetecties.

Malicious NuGet-pakketten leveren tijdvertraging-destructieve payloads

Socket-onderzoekers hebben negen kwaadaardige NuGet-pakketten ontdekt die gebruikmaken van tijdvertragingen om destructieve payloads te leveren. Deze pakketten, gepubliceerd onder de alias shanhai666 tussen 2023 en 2024, kunnen applicaties doen crashen en industriële besturingssystemen verstoren. De kwaadaardige pakketten, waaronder het meest gevaarlijke Sharp7Extend, richten zich op verschillende databasesystemen zoals SQL Server, PostgreSQL en SQLite, evenals industriële PLC's (programmable logic controllers). Het Sharp7Extend-pakket bevat twee sabotagemechanismen: onmiddellijke procesbeëindiging en stille schrijfoperaties die na een vertraging van 30 tot 90 minuten mislukken. De kwaadaardige code heeft 9.488 downloads verzameld en is nog steeds actief, ondanks dat NuGet onderzoek doet naar de verwijdering. Organisaties worden aangespoord om onmiddellijk hun systemen te controleren op deze kwaadaardige pakketten.

Scholen moeten vanaf 2030 voldoen aan normen voor digitale veiligheid

Vanaf 2030 moeten Nederlandse basisscholen en middelbare scholen voldoen aan strikte normen voor digitale veiligheid. Deze normen, die onder andere betrekking hebben op de veilige uitwisseling van privacygevoelige informatie en het omgaan met hacks, worden vastgesteld om de risico's van cyberaanvallen op het onderwijs te verkleinen. Demissionair staatssecretaris Becking benadrukt dat er in 2025 verschillende cyberincidenten plaatsvonden die de continuïteit van het onderwijs in gevaar brachten. Om scholen te ondersteunen, is het programma Digitaal Veilig

Onderwijs (DVO) opgericht, dat samenwerkt met diverse organisaties zoals de PO-Raad en VO-raad. Scholen hebben tot 2030 de tijd om de normen uit het "Normenkader Informatiebeveiliging en Privacy Funderend Onderwijs" te implementeren, met financiële steun van de overheid. De Inspectie van het Onderwijs kan ingrijpen als scholen niet voldoen aan de vereisten.

Britse telecombedrijven nemen maatregelen tegen telefoonspoofing

Britse telecombedrijven hebben nieuwe maatregelen aangekondigd om telefoonspoofing te bestrijden. De maatregelen richten zich op het voorkomen van misleidende telefoongesprekken, zoals bankfraude waarbij oplichters zich voordoen als medewerkers van een bank. De telecomproviders, waaronder BT en Vodafone, zullen hun netwerken upgraden om spoofing door buitenlandse callcenters te blokkeren. Bij gesprekken van dergelijke callcenters wordt het internationale telefoonnummer voortaan aangegeven. Daarnaast wordt er technologie ingezet om verdachte telefoontjes en sms-berichten te blokkeren voordat ze bij eindgebruikers terechtkomen. De telecombedrijven werken ook samen met de politie om data te delen en gesprekken te traceren, wat hen moet helpen bij het opsporen van criminelen. Deze nieuwe maatregelen moeten de impact van oplichtingspraktijken verminderen, aangezien steeds meer mensen geconfronteerd worden met telefoonspoofing.

Rockstar ontslaat medewerkers vanwege lekken bedrijfsgeheimen

Rockstar Games heeft onlangs meer dan dertig medewerkers ontslagen, naar eigen zeggen vanwege het delen van vertrouwelijke bedrijfsinformatie op een online forum. De werknemers zouden zich schuldig hebben gemaakt aan het schenden van interne richtlijnen door geheime gegevens in een openbare Discord-groep te delen. Volgens de vakbond The Independent Workers' Union of Great Britain zouden de ontslagen echter verband houden met het lidmaatschap van de vakbond of de wens om zich aan te sluiten. De vakbond beschouwt deze ontslagen als onwettig, maar Rockstar betwist dit en stelt dat de medewerkers wegens wangedrag zijn ontslagen. Het bedrijf benadrukt dat het ontslag geen verband houdt met vakbondactiviteiten. Rockstar, bekend van onder andere de Grand Theft Auto-reeks, werkt momenteel aan de langverwachte game GTA VI, waarvan de lancering gepland is voor november 2026, na een eerdere uitstel.

Interview met Everest Ransomware Groep over de Collins Aerospace-inbraak

In september 2025 veroorzaakte een cyberaanval chaos in de Europese luchtvaart, waarbij systemen op luchthavens zoals Heathrow, Brussel en Berlijn werden uitgeschakeld. De aanval richtte zich op de MUSE-software van Collins Aerospace, die wordt gebruikt voor passagiersverwerking. Hoewel aanvankelijk ransomware als oorzaak werd genoemd, claimde de Everest Ransomware Groep verantwoordelijk te zijn voor de inbraak. Ze maakten gebruik van gestolen inloggegevens, die eerder in 2022 waren buitgemaakt, en exfiltreerden meer dan 50 GB aan gegevens, waaronder persoonlijke gegevens van passagiers en werknemers. De groep ontkent ransomware te hebben gebruikt en beschuldigt Collins Aerospace van verzekeringsfraude, waarbij ze de servers opzettelijk afsloten om een verzekeringsbetaling te verkrijgen. De Everest Groep benadrukt dat hun focus ligt op het blootleggen van veiligheidsproblemen zonder schade aan infrastructuur aan te richten.