Cybercrimeinfo - cyberdreigingsanalyse (Openbare versie)

22-11-2025:

Google onthult BadAudio-malware die gebruikt wordt in APT24-spionagecampagnes

Google heeft de onthulling gedaan van een malware genaamd BadAudio, die al drie jaar wordt ingezet door APT24, een hackercollectief met banden in China. Deze groep heeft BadAudio gebruikt in een langdurige spionagecampagne die recent is geëvolueerd naar geavanceerdere aanvalsmethoden. APT24 verspreidde de malware via verschillende aanvallen, waaronder spearphishing, supply-chain compromissen en watering hole-aanvallen. De malware werd vaak verspreid via valse software-updates en misbruik van legitieme websites, waarbij JavaScript werd geïnjecteerd om slachtoffers te identificeren en hen naar een kwaadaardige pop-up te leiden.

Vanaf 2024 breidde de groep haar tactieken uit door herhaaldelijk een marketingbedrijf in Taiwan te compromitteren, dat JavaScript-bibliotheken levert aan duizenden andere websites. APT24 injecteerde hierbij malafide JavaScript in veel gebruikte bibliotheken, waardoor meer dan duizend domeinen werden getroffen. In parallelle aanvallen werden ook spearphishing-e-mails gebruikt, die zich voordeden als berichten van dierenreddingsorganisaties en waarbij diensten zoals Google Drive en OneDrive werden misbruikt om de malware te verspreiden.

De BadAudio-malware maakt gebruik van geavanceerde obfuscatie-technieken, waaronder DLL hijacking en een methode genaamd control flow flattening, waardoor het erg moeilijk is voor analisten om de malware te detecteren of te reverse-engineeren. Zodra de malware is uitgevoerd op een slachtoffercomputer, verzamelt het systeeminformatie en stuurt deze versleuteld naar de aanvallers. Vervolgens wordt een payload gedownload en uitgevoerd via een techniek die bekendstaat als DLL sideloading, waardoor het moeilijker is voor beveiligingssoftware om de bedreiging te detecteren.

Deze spionagecampagne is opmerkelijk omdat het de duur van drie jaar overspant en ondanks de opkomst van steeds geavanceerdere detectiemethoden, bleef BadAudio grotendeels onopgemerkt. Slechts een klein aantal samples werd door antivirussoftware opgemerkt, wat de effectiviteit van de aanvalstechnieken van APT24 benadrukt.

Chinese hackers misbruiken kwetsbaarheid in WSUS om ShadowPad malware te verspreiden

Hackers met vermoedelijke Chinese steun maken gebruik van een kritieke kwetsbaarheid in Microsoft Windows Server Update Services (WSUS) om de geavanceerde malware ShadowPad te verspreiden. Deze malware is een backdoor die eerder in verband is gebracht met meerdere door staten gesponsorde groepen. De aanvallen maken gebruik van de kwetsbaarheid CVE-2025-59287, een remote code execution (RCE) fout die aanvallers systeemtoegang geeft tot kwetsbare servers. Sinds de publieke release van een proof-of-concept code in oktober 2025, hebben cybercriminelen deze kwetsbaarheid snel geadopteerd om netwerken van bedrijven met een WSUS-infrastructuur te compromitteren.

De aanval begint wanneer de hackers Windows-servers met WSUS inschakelen en gebruikmaken van de kwetsbaarheid om systeemtoegang te verkrijgen. Nadat ze toegang hebben, implementeren ze PowerCat, een open-source PowerShell-gebaseerd hulpmiddel dat hen direct toegang tot de command shell van het getroffen systeem biedt. Dit eerste toegangspunt stelt de aanvallers in staat om verdere opdrachten uit te voeren voor het installeren van de malware. Tijdens de aanval wordt ShadowPad gedownload en geïnstalleerd met behulp van legitieme Windows-hulpmiddelen zoals certutil en curl, waardoor de kans op detectie wordt verminderd.

ShadowPad maakt gebruik van een techniek genaamd DLL-sideloading, waarbij het niet als een zelfstandige executable draait, maar in plaats daarvan een legitiem Windows-programma zoals ETDCtrlHelper.exe wordt misbruikt om een kwaadaardige DLL te laden. Deze DLL fungeert als een loader voor de ShadowPad-backdoor, die volledig in het geheugen draait. De malware blijft persistent door het maken van services, registerinstellingen en geplande taken, en communiceert met command-and-control-servers via HTTP en HTTPS, waarbij het verkeer wordt gemaskeerd met standaard Firefox-browserheaders.

Organisaties die WSUS gebruiken, wordt dringend geadviseerd om de beveiligingsupdate van Microsoft voor CVE-2025-59287 onmiddellijk toe te passen en serverlogboeken te monitoren op verdachte PowerShell-, certutil- en curl-uitvoeringspatronen om mogelijke pogingen tot compromis te detecteren.

Noord-Koreaanse hackinggroepen Kimsuky en Lazarus bundelen krachten om zero-day kwetsbaarheden wereldwijd te misbruiken

De Noord-Koreaanse hackercollectieven Kimsuky en Lazarus hebben hun krachten gebundeld om een gecoördineerde cyberaanval uit te voeren die organisaties wereldwijd bedreigt. Deze samenwerking markeert een belangrijke verschuiving in de werkwijze van staatsgesponsorde dreigingsactoren, die nu van geïsoleerde aanvallen overgaan naar zorgvuldig geplande en gecoördineerde operaties. Het gezamenlijke doel van deze groepen is het stelen van gevoelige inlichtingen en cryptocurrency, met behulp van een systematische aanpak die sociale manipulatie en zero-day-exploits combineert.

Het aanvallingsproces begint met Kimsuky, dat via phishingmails gericht op academische conferenties of verzoeken om samenwerking informatie verzamelt. Deze e-mails bevatten kwaadaardige bijlagen in HWP- of MSC-formaten die, zodra ze worden geopend, de FPSpy backdoor activeren. Na installatie van deze backdoor wordt een keylogger genaamd KLogEXE geactiveerd, die wachtwoorden, e-mailinhoud en systeeminformatie vastlegt. Dit stelt de aanvallers in staat om het netwerk van de doelwitten te verkennen en waardevolle informatie in kaart te brengen.

Vervolgens neemt Lazarus de controle over de getroffen systemen en maakt gebruik van zero-day-kwetsbaarheden om diepere toegang te verkrijgen. Het exploiteert de CVE-2024-38193, een privilege escalation-bug in Windows, om kwaadaardige Node.js-pakketten te implementeren die op het eerste gezicht legitiem lijken. Zodra deze pakketten worden uitgevoerd, verkrijgen de aanvallers systeemniveau toegang en installeren ze de InvisibleFerret backdoor. Deze malware maakt gebruik van geavanceerde technieken om endpoint-detectie te omzeilen, waardoor het voor beveiligingsteams bijzonder moeilijk is om de activiteit op te sporen.

De InvisibleFerret backdoor is bijzonder geavanceerd, aangezien het netwerkverkeer als reguliere HTTPS-webverzoeken wordt gemaskeerd. Dit maakt het uiterst moeilijk om kwaadaardige activiteit te detecteren door middel van verkeersanalyse. De malware richt zich specifiek op blockchain-wallets door systeemberichten te scannen op privé-sleutels en transactiegegevens die in browserextensies en desktopapplicaties zijn opgeslagen. In een gedocumenteerd geval wisten de aanvallers binnen 48 uur $32 miljoen aan cryptocurrency te verplaatsen zonder beveiligingswaarschuwingen te activeren.

Na het voltooien van hun aanvallen werken de groepen samen om bewijs van hun aanwezigheid te verwijderen door gebruik te maken van gedeelde infrastructuur. Ze overschrijven kwaadaardige bestanden met legitieme systeemprocessen en wissen

aanvallogs. Organisaties in de sectoren defensie, financiën, energie en blockchain lopen de grootste risico's van deze dreiging.

Kritieke kwetsbaarheid in Vue I18n-plugin voor Vue.js ontdekt: mogelijke externe code-uitvoering

Op 20 november 2025 werd een ernstige kwetsbaarheid in de Vue I18n-plugin voor Vue.js bekendgemaakt, die mogelijk kan leiden tot externe code-uitvoering (RCE) door misbruik van objectprototype-attributen. De kwetsbaarheid, gemeld als CVE-2025-27597, heeft betrekking op versies van de plugin die variëren van 9.1.0 tot 9.14.3, evenals enkele versies van de alpha- en beta-fases van Vue I18n 10.x en 11.x. De kwetsbaarheid werd geclassificeerd met een hoge ernst, met een CVSS-score van 8.9, wat wijst op aanzienlijke risico's voor zowel de beschikbaarheid als de integriteit en vertrouwelijkheid van de getroffen systemen.

De oorzaak van de kwetsbaarheid ligt in het onbeheerd verwerken van gebruikersinvoer, die kan leiden tot de wijziging of toevoeging van objecteigenschappen binnen de Vue.js-toepassing. Dit gebeurt wanneer woorden zoals "proto" of "constructor" in vertaalde gegevens worden ingebracht, waardoor eigenschappen op objecten worden aangepast. In sommige gevallen kan dit leiden tot onbedoelde uitvoer van commando's, waardoor kwaadwillende actoren mogelijk toegang krijgen tot kritieke systemen.

Gezien de eenvoud van de exploitatie en de beschikbaarheid van een proof-of-concept (PoC), wordt onmiddellijk patchen aangeraden om verdere schade te voorkomen. Organisaties die kwetsbare versies van Vue I18n gebruiken, wordt sterk geadviseerd de updates met hoge prioriteit te installeren na grondige tests.

Kritiek RCE-lek in Oracle Identity Manager mogelijk misbruikt bij aanvallen

Een ernstige kwetsbaarheid in Oracle Identity Manager, een softwareoplossing voor gebruikersbeheer, heeft mogelijk weken voor het uitkomen van een beveiligingsupdate tot misbruik geleid. Het betreft een remote code execution (RCE) kwetsbaarheid, geïdentificeerd als CVE-2025-61757, die werd gemeld door het bedrijf Searchlight Cyber. Deze kwetsbaarheid kreeg de hoogst mogelijke risicoscore van 9.8 op een schaal van 10. Het lek stelt een aanvaller in staat om op afstand code uit te voeren zonder authenticatie.

Oracle bracht op 21 oktober 2025 beveiligingsupdates uit, die deze kwetsbaarheid moesten verhelpen. Onderzoekers van het Internet Storm Center (ISC) ontdekten in logbestanden van honeypots dat een URL, die verband houdt met de kwetsbaarheid, herhaaldelijk werd bezocht tussen 30 augustus en 9 september 2025. Dit kan wijzen op pogingen om de kwetsbaarheid te misbruiken, hoewel het niet mogelijk was om te bevestigen of deze bezoeken daadwerkelijk werden gebruikt voor misbruik. Het lek in Oracle Identity Manager stelt aanvallers in staat om toegang te krijgen tot gevoelige systemen en mogelijk ernstige gevolgen voor de veiligheid van de getroffen organisaties te veroorzaken.

Grafana waarschuwt voor kwetsbaarheid met maximale ernst in Enterprise-product

Grafana Labs heeft een waarschuwing uitgegeven voor een kwetsbaarheid met maximale ernst in haar Enterprise-product. De kwetsbaarheid, aangeduid als CVE-2025-41115, stelt aanvallers in staat om nieuwe gebruikers ten onrechte als beheerders te behandelen of om priviliges op te schalen. Dit probleem doet zich voor wanneer de SCIM (System for Cross-domain Identity Management) provisioning is ingeschakeld en correct is geconfigureerd.

Om de kwetsbaarheid te kunnen misbruiken, moeten zowel de 'enableSCIM'-featureflag als de optie 'user_sync_enabled' op 'waar' staan. Hierdoor kan een kwaadwillende of gecompromitteerde SCIM-client een gebruiker voorzien van een extern ID dat overeenkomt met een intern account, zoals dat van een beheerder. Dit kan leiden tot het vervalsen van gebruikers of het verkrijgen van verhoogde privileges.

De kwetsbaarheid treft alleen de versies 12.0.0 tot 12.2.1 van Grafana Enterprise wanneer SCIM is ingeschakeld. Grafana OSS-gebruikers zijn niet getroffen, en Grafana Cloud-services hebben reeds patches ontvangen. Grafana adviseert beheerders van zelfbeheerde installaties om snel de beschikbare patches toe te passen, zoals versie 12.3.0 of een van de eerdere versies die de fout verhelpen.

De kwetsbaarheid werd ontdekt tijdens een interne audit op 4 november 2025. Grafana Labs heeft de patch binnen 24 uur uitgebracht, zonder aanwijzingen dat de kwetsbaarheid in Grafana Cloud was misbruikt. Gebruikers wordt dringend aangeraden de beveiligingsupdate toe te passen of de SCIM-configuratie tijdelijk uit te schakelen om verdere misbruik te voorkomen.

ENISA wordt een CVE Root, wat de rol van de EU in het beheer van kwetsbaarheden vergroot

Op 21 november 2025 werd de Europese Unie Agentschap voor Cyberbeveiliging (ENISA) gepromoveerd tot een CVE Root, een belangrijke stap in de ontwikkeling van de Europese benadering van kwetsbaarheidsbeheer. Deze wijziging stelt ENISA in staat een centrale rol te vervullen in de coördinatie van kwetsbaarheidsrapportages, openbaarmaking en grensoverschrijdende reacties binnen de EU. Voorheen was ENISA al een CVE Numbering Authority (CNA), maar met de status van CVE Root heeft de organisatie een veel bredere verantwoordelijkheid gekregen, die verder gaat dan alleen de nationale context.

Het CVE-systeem (Common Vulnerabilities and Exposures) is een wereldwijd erkende lijst van bekende kwetsbaarheden in software en hardware. De CVE Roots zijn de hoogste autoriteiten in dit systeem, die toezicht houden op de nummering van kwetsbaarheden en de naleving van de CVE-regels door andere organisaties, de zogenaamde CVE Numbering Authorities. Met de nieuwe status van ENISA als Root krijgt de organisatie de taak om de processen voor het toewijzen en publiceren van CVE-nummers te stroomlijnen en te verbeteren voor de Europese regio.

Een van de belangrijkste voordelen van deze verandering is de centralisatie van de kwetsbaarheidscoördinatie binnen de EU. Voorheen was de coördinatie vooral afhankelijk van internationale organisaties zoals MITRE en CISA, die niet altijd optimaal afgestemd zijn op de specifieke behoeften van Europese landen. Met ENISA in de hoofdrol kan de EU nu zorgen voor een uniformere aanpak in het beheer van kwetsbaarheden, vooral in gevallen waarin een beveiligingsprobleem meerdere lidstaten beïnvloedt. Dit kan helpen om de snelheid en effectiviteit van de kwetsbaarheidsbehandeling te verbeteren, wat van cruciaal belang is in een steeds complexere cyberdreigingsomgeving.

Een ander belangrijk aspect van ENISA's nieuwe rol is de integratie met twee belangrijke EU-initiatieven: de Europese Kwetsbaarheidsdatabase (EUVD) en het Single Reporting Platform (SRP) onder de Cyber Resilience Act. De EUVD, beheerd door ENISA, is de centrale opslagplaats voor kwetsbaarheidsinformatie binnen de EU en wordt verplicht gesteld door de NIS2-richtlijn. Daarnaast zal het SRP vanaf 2026 fabrikanten verplichten om kwetsbaarheden die actief worden misbruikt, te melden bij ENISA. Deze initiatieven zorgen ervoor dat kwetsbaarheden sneller en

efficiënter kunnen worden gedeeld tussen de EU-lidstaten en de bredere CVE-gemeenschap, wat de algehele respons op cyberdreigingen ten goede zal komen.

Met de nieuwe status van CVE Root kan ENISA ook een belangrijke rol spelen in het verminderen van wereldwijde knelpunten binnen het CVE-systeem. De afgelopen jaren heeft het systeem te maken gehad met vertragingen en inconsistenties in de verwerking van kwetsbaarheidsrapporten, deels door de hoge werkdruk op bestaande Roots. Door ENISA toe te voegen aan dit netwerk, wordt de werklast verdeeld, waardoor er sneller en consistenter kan worden gereageerd op nieuwe kwetsbaarheden.

Samenvattend betekent de promotie van ENISA naar een CVE Root een aanzienlijke versterking van de rol van de EU in het beheer van cyberkwetsbaarheden. Dit is niet alleen een belangrijke stap voor Europese cyberbeveiliging, maar ook een teken van de bredere strategie van de EU om meer autonomie te verkrijgen in het beheer van kwetsbaarheden en compliance binnen de regio.

Achterstanden bij OM door Citrix-hack nog niet opgelost

De demissionaire minister van Justitie en Veiligheid, Van Oosten, heeft bekendgemaakt dat de achterstanden bij het Openbaar Ministerie (OM) als gevolg van de Citrix-hack nog niet zijn weggewerkt. Het incident, dat in juli 2025 plaatsvond, leidde ertoe dat het OM uit voorzorg de interne systemen van het internet loskoppelde. Dit besluit werd genomen nadat het Nationaal Cyber Security Centrum (NCSC) waarschuwde voor mogelijk misbruik van een kwetsbaarheid in Citrix, het platform dat gebruikt werd voor thuiswerken.

De offlinegang van systemen en de langzame herstart zorgden voor vertragingen in de uitvoering van taken bij het OM. Het onvermogen van medewerkers om thuis te werken, verergerde de situatie en had invloed op de werkdruk. Sinds oktober kunnen de meeste medewerkers weer thuiswerken, maar in de tussentijd werkten ze in shifts.

Van Oosten bevestigde dat er sprake was van een verhoogde werkdruk door het incident, wat niet te vermijden was. Er wordt volop gewerkt aan het inhalen van de achterstanden, maar het is nog niet bekend wanneer dit volledig is afgerond. De minister liet ook weten dat een commissie van deskundigen zal onderzoeken hoe het OM heeft gereageerd op de aanval, welke stappen er zijn genomen, welke risico's zijn geïdentificeerd en hoe het herstelproces verloopt.

Valse facturen en nepfoto's van schade: oplichters gebruiken AI voor verzekeringsfraude

In de wereld van verzekeringen neemt de invloed van kunstmatige intelligentie (AI) in zowel frauduleuze als opsporingsprocessen steeds verder toe. Oplichters maken steeds vaker gebruik van AI-technologieën om valse schadeclaims in te dienen, waarbij ze kunstmatig gegenereerde schadefoto's en vervalste facturen presenteren. Deze tactieken maken het voor verzekeraars steeds moeilijker om fraude tijdig te detecteren. Het Verbond van Verzekeraars ontdekte in 2024 ruim 9.000 gevallen van fraude, wat neerkomt op ongeveer 25 incidenten per dag. Dit aantal is gestegen ten opzichte van het vorige jaar, waarbij fraudeurs voor een totale schade van 95,6 miljoen euro probeerden te ontfutselen.

Naast de vervalste documenten, zoals facturen voor dure producten, is ook de inzet van AI voor het genereren van deepfake-video's of spraakberichten zorgwekkend. Dit soort oplichting probeert medewerkers van verzekeringsmaatschappijen te misleiden door hen te laten denken dat ze communiceren met hogere leidinggevenden. Een voorbeeld hiervan was een AI-gegenereerd spraakbericht dat het leek alsof het van een directielid afkomstig was, bedoeld om vertrouwelijke informatie te verkrijgen.

Verzekeraars proberen hierop in te spelen door AI ook zelf in te zetten voor het opsporen van frauduleuze activiteiten. Dit gebeurt bijvoorbeeld door ongebruikelijke patronen te detecteren, zoals het indienen van meerdere claims in korte tijd, of door deepfakes te herkennen. De detectie van dergelijke frauduleuze claims wordt verder ondersteund door het gezamenlijke waarschuwingssysteem, waarin verzekeraars informatie delen over bewezen fraudeurs. Bovendien wordt er steeds meer op het 'niet-pluis-gevoel' van medewerkers vertrouwd om verdachte gevallen vroegtijdig te signaleren.

De groei van AI-gebruik in fraude en opsporing benadrukt zowel de risico's als de mogelijkheden die deze technologie met zich meebrengt voor de verzekeringssector.

Matrix Push C2 gebruikt browsermeldingen voor fileless, cross-platform phishingaanvallen

Malafide actoren maken gebruik van browsermeldingen als aanvalsmiddel voor phishingaanvallen via een nieuwe command-and-control (C2) platform genaamd

Matrix Push C2. Dit browser-native, fileless framework benut web push meldingen, valse waarschuwingen en linkomleidingen om slachtoffers op verschillende besturingssystemen te targeten. Onderzoekers van Blackfog, die dit platform ontdekten, rapporteren dat aanvallers slachtoffers misleiden om browsermeldingen toe te staan op schadelijke of gecompromitteerde websites.

Wanneer een slachtoffer akkoord gaat met het ontvangen van meldingen, gebruiken de aanvallers het ingebouwde web push-mechanisme in de browser om valse meldingen te versturen die lijken te komen van het besturingssysteem of de browser zelf. Deze meldingen kunnen bijvoorbeeld waarschuwingen over verdachte inlogpogingen of browserupdates bevatten, met knoppen zoals "Verifiëren" of "Bijwerken". Wanneer het slachtoffer op zo'n knop klikt, wordt het doorgestuurd naar een valse website die bedoeld is om persoonlijke gegevens of inloggegevens te stelen.

Wat deze techniek bijzonder gevaarlijk maakt, is dat het hele proces via de browser verloopt, zonder dat de aanvaller eerst toegang hoeft te krijgen tot het systeem via traditionele infectiemethoden. Dit maakt de aanval een cross-platform dreiging, omdat elke browser die de schadelijke meldingen ontvangt, deel kan gaan uitmaken van het netwerk van gecompromitteerde systemen. Bovendien kunnen aanvallers deze techniek gebruiken om langzaam het niveau van de aanval te escaleren door andere phishingberichten te sturen, meer persistente malware te installeren of zelfs gebruik te maken van browserkwetsbaarheden voor diepere controle over het systeem.

Matrix Push C2 wordt verkocht als een malware-as-a-service (MaaS) kit via criminele kanalen, zoals Telegram en cybercrimeforums, met abonnementskosten die variëren van $150 voor een maand tot $1.500 voor een jaar. Het platform biedt een webgebaseerd dashboard waarmee aanvallers meldingen kunnen versturen, het gedrag van slachtoffers in realtime kunnen volgen, en aangepaste phishingsjablonen kunnen gebruiken om de geloofwaardigheid van hun berichten te vergroten.

De onderzoekers benadrukken dat het gebruik van webpush-meldingen in deze aanvallen een nieuwe benadering is van hoe aanvallers toegang krijgen tot systemen, met als uiteindelijke doel gegevensdiefstal of het geldelijk uitbuiten van toegang tot systemen, bijvoorbeeld door het leegroven van cryptocurrency-portefeuilles. Deze aanvallen onderstrepen een verschuiving in de manier waarop aanvallers sociale manipulatie gebruiken om gebruikers te misleiden tot het uitvoeren van acties die hun systemen compromitteren.

ToddyCat APT ontwikkelt nieuwe tools voor het stelen van e-maildata uit Outlook

De ToddyCat APT-groep blijft zich ontwikkelen in haar aanvallen op bedrijfsnetwerken, met een focus op het stelen van e-mailgegevens van werknemers binnen doelorganisaties. Het recente onderzoek naar deze aanvallen, uitgevoerd door Kaspersky, heeft nieuwe technieken en tools aan het licht gebracht die door de groep worden ingezet. De aanvallen richten zich specifiek op de beveiliging van e-mailinfrastructuren en het verkrijgen van toegang tot gevoelige bedrijfscommunicatie, zowel via lokale servers als cloudgebaseerde e-maildiensten zoals Microsoft 365.

Een van de gebruikte tools is de nieuwe versie van TomBerBil, die nu ook via PowerShell kan draaien en gericht is op het extraheren van inloggegevens, cookies en wachtwoorden van browsers, inclusief Chrome, Edge en Firefox. Deze tools werden ingezet op domeincontrollers en via het SMB-protocol toegang verkregen tot browserbestanden op gedeelde netwerken. Door de uitvoering op machtige machines in het netwerk kan de ToddyCat-groep toegang krijgen tot een breed scala aan gevoelige gegevens, waaronder opgeslagen wachtwoorden en sessies.

Daarnaast heeft ToddyCat een nieuwe aanvalsmethode geïntroduceerd om toegang te verkrijgen tot offline Outlook-gegevensbestanden, die doorgaans moeilijk te benaderen zijn vanwege de toepassing van encryptie en toegangslimieten in het Outlook-platform. Het aangepaste hulpmiddel TCSectorCopy maakt gebruik van laag-niveau bestandskopieën, waarmee zelfs vergrendelde bestanden van actieve processen kunnen worden gekopieerd. Zodra de OST-bestanden van Outlook zijn gekopieerd, worden ze geëxporteerd met behulp van het XstReader-hulpmiddel, waarmee de aanvallers toegang krijgen tot e-mailcorrespondentie en bijlagen.

Een andere opvallende techniek die door de ToddyCat-groep wordt ingezet, is het verkrijgen van OAuth 2.0-toegangstokens uit de Outlook- en Microsoft 365-processen. Deze tokens worden rechtstreeks uit het geheugen van de betrokken applicaties gehaald, waardoor de aanvallers in staat zijn om e-mailgegevens op te vragen zonder dat ze rechtstreeks toegang hoeven te krijgen tot de onderliggende infrastructuur. Dit proces wordt uitgevoerd met behulp van het SharpTokenFinder-hulpmiddel, waarmee toegangstokens snel kunnen worden gedumpt en gedeeld via een SMB-verbinding.

Deze geavanceerde aanvalstechnieken vereisen zorgvuldige monitoring en detectie. Aanbevolen wordt om netwerkanalyses en bestandsaccesscontrole uit te voeren, evenals specifiek toezicht te houden op toegangspogingen tot gevoelige e-mailbestanden en encryptiesleutels. De ToddyCat-groep blijft een ernstige bedreiging voor organisaties die afhankelijk zijn van e-mail en cloudgebaseerde diensten voor hun bedrijfsvoering, en het is essentieel dat deze methoden nauwlettend worden gevolgd om potentiële schade te minimaliseren.

Ransomware-aanvallen richten zich op retailers tijdens het hoogtepunt van het winkelseizoen

Retailers worden momenteel geconfronteerd met een sterke stijging van ransomware-aanvallen nu het winkelseizoen op zijn hoogtepunt is. Deze aanvallen zijn zorgvuldig getimed om samen te vallen met de piek in de verkoop, wanneer de druk om betalingen te doen en de gevolgen van uitvaltijd het grootst zijn. De aanvallers richten zich vooral op netwerken van verkooplocaties, e-commerce backends en ondersteunende IT-systemen die bestellingen, loyaliteitsgegevens en betalingsverwerkingen beheren.

De cybercriminelen maken gebruik van een mix van phishing-e-mails, nep-verzendbevestigingen en schadelijke advertenties die gebruikers naar exploitkits leiden. Zodra een slachtoffer op een link klikt, verplaatst de aanval zich snel van de eerste toegang tot een volledige domeincompromittering. Het uiteindelijke doel is het inzetten van versleutelde bestandspayloads en tools voor gegevensdiefstal in een gecoördineerde aanval, vaak binnen enkele uren na de eerste toegang.

De malware die wordt ingezet, maakt gebruik van een lichtgewicht loader die via een schadelijke bijlage of script wordt gedownload. Deze loader injecteert zich in vertrouwde processen zoals explorer.exe of powershell.exe om eenvoudige detectieregels te omzeilen. Vervolgens haalt de malware de hoofdpayload op van een server die door de aanvaller wordt beheerd, via HTTPS-verkeer dat wordt gemaskeerd als legitieme cloud- en CDN-domeinen. De malware verzamelt vervolgens inloggegevens van het LSASS-proces en gecachte browsersessies, waarna deze zich via bestaande netwerkroutes verspreidt over de systemen van de winkel en de point-of-sale (POS)-systemen.

Deze aanvallen veroorzaken aanzienlijke schade, doordat voorraadbeheersystemen worden versleuteld, betaalterminals worden geblokkeerd en online bestelplatforms

onbereikbaar worden, wat zowel fysieke als digitale verkopen stillegt. Naast de versleuteling van gegevens loopt de retailer ook het risico op gegevensdiefstal, waaronder klantgegevens en interne prijs- of promotieplannen, wat de dreiging van dubbele afpersing en mogelijke boetes door toezichthouders vergroot.

Deze gerichte aanvallen benadrukken het belang van robuuste beveiligingsmaatregelen, vooral tijdens het drukke verkoopseizoen, om de continuïteit van de bedrijfsvoering te waarborgen en de risico's voor klantgegevens te minimaliseren.

Operation DreamJob: Cyberaanval op de maakindustrie via WhatsApp Web-berichten met valse vacature-aanbiedingen

In augustus 2025 werd een geavanceerde cyberaanval uitgevoerd op een Aziatische vestiging van een grote Europese fabrikant. Deze aanval, geïdentificeerd als "Operation DreamJob", maakt gebruik van verfijnde social engineering-technieken om werknemers binnen de maakindustrie te misleiden en toegang te verkrijgen tot bedrijfsnetwerken. De aanvallers gebruikten WhatsApp Web-berichten die zich voordeden als jobgerelateerde documenten om malware te verspreiden.

Het aanvallen begon met een projectingenieur die een bericht ontving via WhatsApp Web, waarin een ogenschijnlijk legitiem werkgerelateerd bestand werd aangeboden. Het bestand was een ZIP-archief, waarin een kwaadaardige PDF, een legitieme open-source applicatie genaamd SumatraPDF.exe, en een kwaadaardige DLL-bestand met de naam libmupdf.dll waren verpakt. Door een techniek genaamd DLL-sideloading werd de onschuldige SumatraPDF.exe gebruikt om de kwaadaardige DLL te laden, wat leidde tot de uitvoering van de malware op het systeem van het slachtoffer.

Onderzoek door Orange Cyberdefense onthulde dat de aanval waarschijnlijk werd uitgevoerd door de Noord-Koreaanse dreigingsgroep UNC2970. De aanvallers maakten gebruik van malwarevarianten zoals BURNBOOK en MISTPEN, en maakten gebruik van kwetsbare SharePoint- en WordPress-infrastructuren voor hun command-and-control-operaties. Na de initiële toegang via de kwaadaardige PDF, werden er verdere technieken ingezet om door het netwerk te bewegen, waaronder het uitvoeren van LDAP-query's op de Active Directory om gebruikers en computers te enumereren en vervolgens administratieve accounts over te nemen met behulp van pass-the-hash-aanvallen.

De dreiging breidde zich verder uit met het gebruik van een extra payload genaamd TSVIPsrv.dll, een variant van de MISTPEN-backdoor. Deze backdoor stelde de aanvallers in staat om verbindingen te maken met gecompromitteerde SharePoint-servers voor verdere communicatie en gegevensdiefstal. De laatste fase van de aanval was het implementeren van Release_PvPlugin_x64.dll, een informatie-stelende module die bedoeld was om gevoelige gegevens van de geïnfecteerde systemen te exfiltreren.

De Operation DreamJob-aanval benadrukt de toenemende verfijning van sociale-engineering-aanvallen gericht op de maakindustrie en de kracht van WhatsApp Web als vector voor het verspreiden van malware. Het incident onderstreept de voortdurende noodzaak voor bedrijven om waakzaam te blijven voor geavanceerde aanvalstechnieken en om het bewustzijn van cyberdreigingen onder hun personeel te vergroten.

Xillen Stealer met nieuwe geavanceerde functies omzeilt AI-detectie en steelt gevoelige gegevens van wachtwoordmanagers

Xillen Stealer, een geavanceerd Python-gebaseerd informatie-steler, heeft zich gepositioneerd als een belangrijke dreiging in het landschap van cybercriminaliteit. Oorspronkelijk geïdentificeerd door Cyfirma in september 2025, is deze malware geëvolueerd naar versies 4 en 5, die een arsenaal aan gevaarlijke functies introduceert om gevoelige gegevens, zoals inloggegevens, cryptocurrency-wallets en systeeminformatie, te stelen. De nieuwste versies van de malware richten zich op meer dan 100 browsers en meer dan 70 cryptocurrency-wallets, waarmee het een uitgebreide tool voor het verzamelen van inloggegevens vormt.

Xillen Stealer wordt gepromoot via Telegram-kanalen en heeft een professionele interface waarmee aanvallers de verzamelde data kunnen beheren, infecties kunnen volgen en instellingen kunnen inzien. De malware richt zich niet alleen op browsergegevens, zoals geschiedenis, cookies en opgeslagen wachtwoorden, maar ook op wachtwoordmanagers zoals OnePass, LastPass, BitWarden en Dashlane. Daarnaast steelt het ontwikkelaarsgegevens, cloudconfiguraties van platforms zoals AWS, GCP en Azure, evenals SSH-sleutels en databaseverbindingsinformatie.

Een zorgwekkend aspect van Xillen Stealer is de geavanceerde mogelijkheid om detectie door moderne beveiligingssystemen te omzeilen. De malware maakt gebruik van een module genaamd AIEvasionEngine, die verschillende technieken toepast,

zoals gedragsmimicry, ruisinjectie, willekeurige vertragingen en het verbergen van bronnen om gedragsclassificatoren te verwarren. Daarnaast verandert de Polymorphic Engine de code door instructies te vervangen, controle-stromen te obfuscaten en dode code in te voegen, waardoor elke sample uniek lijkt en handtekeninggebaseerde detectie voorkomt.

Xillen Stealer maakt gebruik van een peer-to-peer command-and-control-structuur die blockchain-transacties inzet, netwerken zoals Tor en I2P anoniem houdt, en gedistribueerde bestandssystemen gebruikt voor dataverkeer. Het verzamelt gestolen gegevens in HTML- en TXT-rapporten en stuurt deze naar de Telegram-accounts van de aanvallers. De combinatie van diefstal van inloggegevens, het omzeilen van detectie en adaptieve targeting maakt deze malware tot een aanzienlijke bedreiging voor zowel individuele gebruikers als zakelijke omgevingen.

AI-gebaseerde gemaskeerde kwaadaardige apps ontwijken AV-detectie om schadelijke payloads te verspreiden

Een nieuwe golf van kwaadaardige Android-applicaties, die zich voordoen als een populaire Koreaanse bezorgservice, heeft de aandacht getrokken van beveiligingsexperts. Deze apps maken gebruik van geavanceerde technieken voor obfuscatie die door kunstmatige intelligentie worden aangedreven. Het doel van deze apps is om traditionele antivirussoftware te omzeilen, terwijl ze tegelijkertijd gevoelige gebruikersinformatie stelen.

De aanvallers achter deze campagne maken gebruik van een slim afleveringsmechanisme waarbij de kwaadaardige apps zich vermommen als legitieme pakketvolg-applicaties. Wanneer gebruikers de benodigde machtigingen verlenen, toont de app een interface die lijkt op die van de echte bezorgservice door verbinding te maken met echte trackingwebsites via willekeurig gegenereerde trackingnummers. Deze sociale-engineeringaanpak wekt vertrouwen bij de gebruikers, terwijl de app op de achtergrond schadelijke activiteiten uitvoert.

Beveiligingsonderzoekers ontdekten dat de kwaadaardige apps AI-gestuurde obfuscatie gebruiken om de functionaliteit te verbergen, waardoor het reverse-engineeren van de code veel moeilijker wordt. De applicatie maakt gebruik van ProGuard-obfuscatie, waarbij alle class-namen, functienaam- en variabelen geïdentificeerd door willekeurige Koreaanse tekststrings worden vervangen. Deze

aanpak maakt patroonherkenning voor geautomatiseerde beveiligingstools aanzienlijk lastiger, wat de detectie van de malware bemoeilijkt.

Daarnaast blijken de kwaadaardige apps gegevens van besmette apparaten uit te voeren via gecompromitteerde legitieme websites die dienstdoen als command-and-control (C2)-servers. De servers zijn moeilijk te detecteren, omdat ze zich voordoen als onschuldige webverkeer, waardoor het gegevensdiefstalproces buiten het zicht van netwerkmonitoringsystemen blijft. Het onderzoek identificeerde vijf bevestigde MD5-hashes en gerelateerde URL's die verwijzen naar gecompromitteerde Koreaanse domeinen die voor data-exfiltratie worden gebruikt.

Deze geavanceerde aanvallen benadrukken het groeiende gebruik van AI voor zowel het maskeren van schadelijke activiteiten als het verbeteren van de effectiviteit van cyberaanvallen. De beveiligingsgemeenschap moet deze dreigingen serieus nemen en proactief maatregelen nemen om deze aanvallen te detecteren en tegen te gaan.

Nieuwe Android-malware biedt volledige spionagecapaciteiten aan cybercriminelen

Een nieuwe vorm van malware voor Android-apparaten, genaamd RadzaRat, heeft de aandacht getrokken van beveiligingsexperts vanwege zijn geavanceerde functionaliteiten en het vermogen om apparaten op afstand te monitoren en te beheren. RadzaRat is een zogenoemde remote access trojan (RAT) die zich voordoet als een legitieme bestandsbeheerder, maar in werkelijkheid cybercriminelen volledige toegang geeft tot het slachtofferapparaat. Dit malwareprogramma stelt aanvallers in staat om niet alleen bestanden te beheren, maar ook toetsaanslagen vast te leggen (keylogging), bestanden tot 10 gigabyte te downloaden, en continue surveillance uit te voeren.

Wat RadzaRat bijzonder gevaarlijk maakt, is het feit dat het geen detectie heeft in beveiligingssystemen. Op VirusTotal, een bekende virusscanner, wordt de malware nog niet herkend door geen enkele van de 66 gebruikte beveiligingsoplossingen. Dit is te wijten aan het feit dat RadzaRat pas recent is opgedoken, op 8 november 2025. Dit betekent dat er een periode is waarin aanvallers het malwareprogramma kunnen inzetten voordat de beveiligingssoftware zich aanpast.

De malware wordt gepromoot via ondergrondse cybercrime-forums en is bijzonder aantrekkelijk voor aanvallers vanwege de relatief lage technische vereisten en het gebruik van gratis infrastructuurdiensten, zoals servers die worden gehost op

Render.com en communicatie via Telegram-bots. De ontwikkelaar van RadzaRat, opererend onder het alias "Heron44", biedt de software aan als een eenvoudige oplossing voor het verkrijgen van toegang op afstand tot Android-apparaten, zonder dat diepgaande technische kennis vereist is.

Een ander zorgwekkend aspect van RadzaRat is de manier waarop het gebruik maakt van het Android Accessibility Service Framework. Dit systeem, oorspronkelijk ontworpen om mensen met een beperking te helpen, wordt door de malware misbruikt om toegang te krijgen tot persoonlijke informatie zonder dat root-toegang nodig is. De malware kan ook systeemrechten verkrijgen via een MyDeviceAdminReceiver-component, waardoor het zich moeilijker kan laten verwijderen door de gebruiker.

Experts waarschuwen dat de risico's niet alleen bestaan voor mensen die applicaties installeren van onbekende bronnen, maar dat zelfs apps die afkomstig zijn van de officiële Google Play Store gevaarlijk kunnen zijn als ze onterecht uitgebreide machtigingen vragen. Het is belangrijk om voorzichtig te zijn bij het verlenen van toestemming voor toegang tot de toegankelijkheidsservice of administratorrechten, zelfs voor apps die ogenschijnlijk legitiem zijn.

Hoewel RadzaRat momenteel nog in ontwikkeling is en versies van het programma mogelijk blijven verbeteren, is het duidelijk dat het een aanzienlijke bedreiging vormt voor Android-gebruikers. De combinatie van publieke beschikbaarheid en de mogelijkheid om detectie te vermijden maakt deze malware bijzonder schadelijk. Het is dan ook van cruciaal belang voor gebruikers om alert te blijven en voorzichtig te zijn met het installeren van apps, zelfs als ze afkomstig zijn van betrouwbare platformen.

Crypto-witwassen in het VK ondersteunt Russische invasie

De Britse politie heeft een uitgebreid netwerk van crypto-witwassen ontdekt, dat Rusland helpt om Westerse sancties te omzeilen en fondsen naar de oorlog in Oekraïne te sturen. Dit netwerk, dat actief is in het VK, maakte gebruik van honderden koeriers om criminele opbrengsten van activiteiten zoals drugshandel en wapenhandel te verzamelen. De opbrengsten werden snel omgezet in cryptocurrency en wereldwijd verplaatst. In de tweede fase van "Operation Destabilise" zijn 128 mensen gearresteerd, en is meer dan 25 miljoen pond aan contanten en cryptocurrencies in beslag genomen. Het onderzoek heeft ook geleid

tot inbeslagnames in andere landen, waarbij buitenlandse partners geholpen werden met inbeslagnames van 24 miljoen dollar en 2,6 miljoen euro. De connectie tussen georganiseerde misdaad, cybercriminaliteit en de Russische militaire-industrie werd duidelijk, met Keremet Bank in Kirgizië als tussenpersoon voor het verplaatsen van de fondsen naar Rusland.

Inbeslagnames tijdens actieweek tegen bezit kinderpornografie

In de periode van 17 tot en met 20 november 2025 heeft de politie in Nederland deelgenomen aan een intensieve actieweek tegen het bezit van kinderpornografie. Gedurende deze week zijn ruim dertig mensen bezocht, waarbij de politie nadere onderzoeken heeft uitgevoerd. Deze bezoeken resulteerden in de inbeslagnames van minimaal 87 digitale gegevensdragers. Op een van de bezochte locaties werden bovendien analoge fotoboeken met kinderpornografische afbeeldingen aangetroffen, die eveneens in beslag zijn genomen.

De actieweek had als doel vroegtijdig in te grijpen en betrokkenen bewust te maken van de ernstige gevolgen van het bezit, downloaden en verspreiden van kinderpornografie. Tijdens de bezoeken heeft de politie met de verdachten gesproken en hen gewaarschuwd voor hun gedrag. Meer dan twintig personen kregen een confrontatiegesprek en werd nadrukkelijk gevraagd te stoppen met het downloaden van kinderpornografie. Tevens werd hen de mogelijkheid geboden om hulp te zoeken via de organisatie Stop it Now, die ondersteuning biedt aan mensen die zich zorgen maken over hun seksuele gevoelens en gedrag richting minderjarigen.

De politie heeft benadrukt dat bij vervolgincidenten opsporingsonderzoeken zullen worden ingesteld. Deze preventieve benadering is onderdeel van een bredere strategie van het Team Bestrijding Kinderpornografie en Kindersekstoerisme (TBKK), dat streeft naar een veilige opgroeiomgeving voor kinderen, vrij van seksueel misbruik. Het TBKK werkt samen met verschillende teams van wijkagenten en heeft aangegeven dat deze vroegtijdige interventies noodzakelijk zijn om ernstigere misdrijven te voorkomen. De actie heeft geleid tot positieve reacties van ouders die beter bewust zijn van de online activiteiten van hun kinderen en zich nu meer verantwoordelijk voelen voor hun digitale veiligheid.

De machtige drugs- en cybercrimineel Sjef R. (44) leeft in een luxewereld

Sjef R., een belangrijke speler in de georganiseerde misdaad, is momenteel voortvluchtig en verblijft in Dubai. Het Openbaar Ministerie (OM) heeft een gevangenisstraf van 20 jaar geëist voor zijn betrokkenheid bij een internationaal drugsimperium en cybercriminaliteit. R. staat bekend om zijn rol in het faciliteren van versleutelde communicatie voor andere criminelen, wat zijn invloed in de wereld van cybercriminaliteit vergroot.

Naast zijn activiteiten in de drugshandel, zou R. betrokken zijn bij geavanceerde cybercriminelennetwerken, waarbij hij digitale middelen gebruikte om zijn operaties wereldwijd te coördineren. Het proces tegen hem loopt echter het risico vast te lopen door juridische complicaties, voornamelijk met een medeverdachte, wat de opsporing bemoeilijkt.

De zaak onderstreept de groeiende uitdaging voor internationale wetshandhavers bij het aanpakken van cybercriminaliteit, vooral wanneer de verdachten zich bevinden in landen met beperkte uitleveringsverdragen, zoals Dubai.

Criminelen rekruteren kinderen via videogames en zetten hen aan tot moord

Europol heeft gewaarschuwd voor een nieuwe vorm van criminele activiteiten waarbij kinderen via videogames en sociale media worden gerekruteerd voor gewelddadige misdaden, waaronder moord. Criminele netwerken manipuleren jongeren door hen eerst in vertrouwen te nemen via onschuldige gesprekken over alledaagse onderwerpen, zoals huisdieren of school. Na het opbouwen van dit vertrouwen worden de kinderen vaak verleid om persoonlijke gegevens te delen en later onder druk gezet om gewelddadige daden uit te voeren, soms zelfs met de dreiging van geweld tegen hun eigen familieleden.

Catherine De Bolle, directeur van Europol, noemt deze trend de grootste criminele bedreiging voor Europa. Ze benadrukt dat de rekrutering van kinderen steeds meer geavanceerd wordt, waarbij zij niet alleen worden gebruikt voor kleine misdaden, maar voor grootschalig geweld. In sommige gevallen worden kinderen zelfs verleid met grote geldbedragen om extreem gewelddadige opdrachten uit te voeren, zoals moord of zelfmoord. Hoewel de meeste van deze pogingen mislukken door de onervarenheid van de kinderen, is het aantal geslaagde gevallen zorgwekkend, met ten minste tien huurmoorden die zijn uitgevoerd door minderjarigen.

Europol wijst erop dat kwetsbare kinderen, zoals degenen die psychische problemen ervaren of slachtoffer zijn van pesterijen, vaak doelwitten zijn, maar ook gezonde en

gelukkige kinderen kunnen slachtoffer worden. De dreiging wordt verder versterkt door de opkomst van kunstmatige intelligentie, die online criminaliteit mogelijk maakt en versterkt.

De Bolle waarschuwt dat als deze trend zich doorzet, de gevolgen voor de toekomst van Europa ernstig kunnen zijn. De manipulatie van kinderen is volgens haar een cruciaal onderdeel van hybride dreigingsstrategieën die niet alleen crimineel, maar ook staatsgesponsord kunnen zijn.

Moderatoren van criminele online groepen veroordeeld voor betrokkenheid bij kindermisbruik

Bradley Talbot, een 29-jarige man uit Portsmouth, is recent veroordeeld voor zijn actieve rol in een criminele online groep die via Telegram kinderen misbruikte. De groep, die meer dan 6.000 leden telde, was betrokken bij het dwingen van kinderen tot het maken van indecente beelden en het afpersen van slachtoffers om zichzelf te schaden. Deze "Com groepen" zijn een groeiend probleem in de wereld van cybercriminaliteit, waarbij deelnemers via internet gezamenlijk misdrijven plegen, variërend van cyberaanvallen tot het verspreiden van materiaal van kindermisbruik.

Talbot, die als moderator fungeerde, was actief betrokken bij het aantrekken van nieuwe leden en het bevorderen van de verspreiding van misbruikmateriaal. De slachtoffers, kinderen tussen de 12 en 17 jaar, werden benaderd via sociale media, waarna hen steeds explicietere en gewelddadigere verzoeken werden gedaan. De groep gebruikte afpersing, waarbij slachtoffers werden bedreigd met het openbaar maken van hun beelden, en in sommige gevallen werd van hen geëist dat ze de namen van hun beulen in hun lichaam sneden.

Dit geval benadrukt de toenemende dreiging van georganiseerde criminele netwerken die gebruikmaken van versleutelde communicatieplatforms zoals Telegram om hun misdaden uit te voeren. De National Crime Agency (NCA) werkte samen met de politie van Hampshire en de Crown Prosecution Service om Talbot op te sporen en voor de rechter te brengen. Hij werd veroordeeld tot zeven jaar en zes maanden gevangenisstraf, met een levenslange seksuele schadepreventieorde (SHPO).

De veroordeling van Talbot maakt duidelijk hoe georganiseerde misdaadgroepen via het internet kwetsbare kinderen kunnen misbruiken en exploiteren. Deze groepen maken gebruik van geavanceerde technieken, zoals versleuteling en anonieme

communicatie, om hun activiteiten te verbergen en nieuwe slachtoffers te werven. De inzet van de NCA en andere opsporingsinstanties toont het belang van samenwerking en geavanceerde technologieën om dergelijke netwerken te ontmantelen.

Daarnaast werd een ander lid van de groep, Thomas Govan, in 2024 gearresteerd en veroordeeld tot 20 jaar gevangenisstraf na schuld te hebben bekend aan meerdere aanklachten, waaronder verkrachting en het maken van kinderpornografie. De zaak van Talbot onderstreept de noodzaak voor waakzaamheid en bescherming tegen cybercriminaliteit, vooral als het gaat om de veiligheid van kinderen op sociale mediaplatforms.

De zaak toont ook de risico's van het ongereguleerde gebruik van communicatie-apps en sociale media voor criminele doeleinden. Het is van groot belang dat zowel ouders, opvoeders als technologiebedrijven zich bewust zijn van deze gevaren en preventieve maatregelen nemen om kinderen te beschermen tegen online misbruik en afpersing.

Hacker claimt 2,3TB aan gegevens gestolen van Italiaanse spoorweggroep Almaviva

Een hacker heeft geclaimd 2,3 terabyte aan gegevens te hebben gestolen van de Italiaanse spoorwegoperator FS Italiane, nadat een aanval plaatsvond op de IT-dienstenprovider Almaviva. De gelekte data werd gepubliceerd op een dark web-forum, en de inhoud zou vertrouwelijke documenten en gevoelige bedrijfsinformatie omvatten. Almaviva, een grote speler in de IT-sector, biedt wereldwijd software-ontwerpen, systeemintegratie, IT-consultancy en CRM-oplossingen aan en heeft wereldwijd ongeveer 41.000 medewerkers.

De getroffen spoorweggroep, FS Italiane, is een staatsbedrijf dat jaarlijks meer dan 18 miljard dollar aan omzet genereert en verantwoordelijk is voor het beheer van de spoorweginfrastructuur in Italië, evenals voor het vervoer van passagiers en goederen. De gebroken beveiliging bij Almaviva heeft niet alleen impact gehad op FS, maar de gevolgen voor andere klanten zijn momenteel onbekend. Het lek bevat volgens experts documenten die recent zijn, inclusief gegevens van het derde kwartaal van 2025, en omvatten contracten met publieke entiteiten, HR-archieven, boekhoudgegevens en technische documentatie.

Almaviva bevestigde de aanval en verklaarde dat de getroffen systemen sindsdien geïsoleerd zijn en dat de benodigde beveiligingsmaatregelen zijn getroffen. De Italiaanse autoriteiten, waaronder de nationale cybersecurityorganisatie en de politie, zijn ingelicht en er loopt een onderzoek naar het incident. Almaviva heeft aangegeven dat het bedrijf blijft samenwerken met de overheid om de situatie verder te onderzoeken en transparant updates te verstrekken. Momenteel is het niet duidelijk of persoonlijke gegevens van passagiers zijn betrokken bij de datalek.

Helft van Nederlands OM stuurt brandbrief over gebrekkige ICT-infrastructuur

Ongeveer 3.000 medewerkers van het Nederlandse Openbaar Ministerie (OM) hebben een brandbrief gestuurd naar de top van de organisatie, waarin zij wijzen op ernstige tekortkomingen in de ICT-infrastructuur. De ondertekenaars, die samen de helft van het personeelsbestand uitmaken, waarschuwen voor de potentiële risico's die deze gebreken met zich meebrengen. De medewerkers vrezen dat de gebrekkige systemen kunnen leiden tot fouten in strafzaken, vertragingen en zelfs de ondermijning van het vertrouwen in de rechtsstaat.

De problemen worden toegeschreven aan jarenlange onderinvesteringen en bezuinigingen, en zouden los staan van de hack die het OM eerder dit jaar trof via een kwetsbaarheid in Citrix. Het herstel van de systemen na de hack duurde weken, maar de structurele ICT-problemen blijven bestaan. De brandbrief benadrukt de noodzaak van een investering in een robuuste digitale infrastructuur voor het OM, om zo de integriteit van het rechtsproces en de veiligheid van de digitale systemen te waarborgen.

Deze situatie benadrukt de kwetsbaarheid van overheidsinstellingen voor zowel interne ICT-problemen als externe dreigingen, wat de noodzaak onderstreept van voortdurende investeringen in cybersecurity en digitale weerbaarheid.

Expert pleit voor standaardblokkade van al het uitgaand netwerkverkeer

Beveiligingsexpert Kevin Beaumont stelt dat organisaties hun netwerk zo moeten inrichten dat al het uitgaande verkeer standaard wordt geblokkeerd en alleen expliciet wordt toegestaan via gecontroleerde kanalen, zoals webproxies of applicatiebewuste firewalls. Aanleiding voor zijn opmerkingen is de ransomwareaanval op de Britse dienstverlener Capita, waarbij aanvallers erin

slaagden ongeveer 1 terabyte aan zeer gevoelige gegevens van miljoenen betrokkenen te exfiltreren en systemen te versleutelen. De Britse privacytoezichthouder ICO legde Capita hiervoor een miljoenenboete op vanwege ernstige tekortkomingen bij de bescherming van persoonsgegevens.

Volgens de reconstructie begon het incident met het onbedoeld downloaden van een malafide JavaScript-bestand op het systeem van een medewerker. Binnen enkele minuten genereerde dit een hooggeprioriteerde waarschuwing in het Security Operations Centre (SOC), maar het betreffende systeem werd pas na tientallen uren daadwerkelijk in quarantaine geplaatst. Uit de bevindingen blijkt dat het SOC structureel onderbemand was en eigen SLA-doelen zelden haalde. Tijdens het incident was slechts één SOC-medewerker actief, wat bijdroeg aan de vertraagde reactie.

Later onderzoek maakte duidelijk dat de aanvallers toegang kregen tot grote hoeveelheden gevoelige data, waaronder informatie over crimineel verleden, politieke opvattingen, seksuele geaardheid, vakbondslidmaatschap en geloofsovertuiging. In eerste instantie stelde Capita dat er geen aanwijzingen waren voor datadiefstal, maar die mededeling bleek onjuist. Beaumont verwijst naar deze gang van zaken als voorbeeld van zowel gebrekkige technische maatregelen als tekortschietende communicatie richting toezichthouder en betrokkenen.

In zijn analyse wijst Beaumont op het ontbreken van effectieve beheersing van uitgaand verkeer. Hij benadrukt dat het niet nodig is dat willekeurige servers grote hoeveelheden data, bijvoorbeeld via tools als rclone, naar onbeperkte internetadressen kunnen versturen. Volgens hem zouden firewall-logs actief op dergelijke patronen moeten worden gecontroleerd en zouden bepaalde tools standaard geblokkeerd moeten worden om grootschalige exfiltratie te bemoeilijken. Hij verwerpt daarbij wat hij omschrijft als een “zero trust-fabel”, omdat volgens hem in de praktijk het uitgaande verkeer vaak nog te weinig wordt beperkt.

Daarnaast formuleert Beaumont een aantal pijlers waarop organisaties zich zouden moeten richten. Zo noemt hij een voldoende bemand en effectief opererend SOC als essentieel onderdeel van de detectie- en responscapaciteit. Verder benadrukt hij het in kaart brengen van systemen die grote hoeveelheden persoonsgegevens bevatten, inclusief het uitvoeren van penetratietesten om de weerbaarheid van deze omgevingen te toetsen. Ook pleit hij ervoor om de beveiliging van Microsoft Active Directory door een externe partij te laten beoordelen, gezien de centrale rol van deze technologie in veel netwerkarchitecturen.

Beaumont onderstreept daarnaast het belang van een organisatiebrede “cybersecuritycultuur”, waarin medewerkers zich bewust zijn van risico’s en incidenten serieus worden genomen. Tot slot wijst hij op de noodzaak om plannen en technische controls regelmatig te testen, zodat duidelijk wordt hoe een organisatie in de praktijk reageert op een aanvalsscenario. De casus Capita wordt door hem gebruikt als illustratie van wat er mis kan gaan wanneer signalen niet tijdig worden opgevolgd, uitgaand verkeer onvoldoende wordt begrensd en communicatie over een incident niet direct en volledig is.

Tweede Kamer bezorgd over DigiD door overname van Solvinity door Amerikaanse partij

Er is groeiende bezorgdheid in de Tweede Kamer over de toekomst van belangrijke Nederlandse overheidsdiensten zoals DigiD en MijnOverheid, nu het cloudbedrijf Solvinity, dat deze diensten ondersteunt, mogelijk in Amerikaanse handen komt. Het Nederlandse bedrijf levert de infrastructuur voor deze vitale systemen, en de overname heeft politieke en veiligheidsrisico's opgeworpen, met name rondom de bescherming van persoonsgegevens en de controle over kritieke digitale diensten.

De vrees is dat met de overname van Solvinity door een Amerikaanse partij, essentiële Nederlandse overheidsdiensten onder buitenlandse invloed zouden kunnen komen te staan. DigiD, een dienst die gebruikt wordt voor identificatie in overheidszaken, is een van de belangrijkste systemen die nu op Solvinity's infrastructuur draait. Daarnaast is ook het beveiligde communicatiesysteem van het ministerie van Justitie en Veiligheid afhankelijk van dezelfde infrastructuur.

GroenLinks-PvdA en de SGP hebben Kamervragen gesteld over de overname en de impact daarvan op de nationale veiligheid en digitale soevereiniteit. De SGP vraagt of er mogelijkheden zijn om de overname tegen te houden, of voorwaarden te stellen om de veiligheid en onafhankelijkheid van deze cruciale digitale infrastructuur te waarborgen. Ook wordt er gevraagd naar de juridische mogelijkheden om de eigendomsstructuur van deze systemen te beschermen tegen buitenlandse controle.

De zorgen gaan verder dan deze specifieke overname. Er wordt aangedrongen op meer concrete stappen om de digitale autonomie van de Nederlandse overheid te versterken, bijvoorbeeld door te investeren in een nationale of "soevereine" overheidscloud. Dit zou ervoor moeten zorgen dat essentiële overheidsdiensten niet

afhankelijk worden van buitenlandse partijen, wat risico's met zich meebrengt op het gebied van gegevensbeveiliging en digitale onafhankelijkheid.

Het kabinet is nu bezig met het evalueren van de juridische en operationele implicaties van de overname. Er wordt verwacht dat staatssecretaris Van Marum over drie weken met een reactie komt. De uiteindelijke beslissing kan verregaande gevolgen hebben voor de controle over burgerdata en de beveiliging van online overheidsdiensten.

SEC laat rechtszaak tegen SolarWinds vallen na juridische stappen

De Amerikaanse Securities and Exchange Commission (SEC) heeft besloten de rechtszaak tegen SolarWinds en de chief information security officer (CISO) van het bedrijf te beëindigen, zonder verdere toelichting. De aanklachten waren gericht op vermeende misleiding van investeerders met betrekking tot de cybersecurity van SolarWinds. Het softwarebedrijf, bekend van de Orion-software die wereldwijd door tienduizenden organisaties wordt gebruikt voor it-beheer, werd beschuldigd van het bagatelliseren van risico's en het onvoldoende informeren over kwetsbaarheden in hun systemen.

In 2020 werd ontdekt dat hackers via geïnfecteerde software-updates de systemen van klanten konden binnendringen. Dit leidde tot een enorme schending van de cybersecurity, waarbij 18.000 klanten getroffen werden. Ondanks waarschuwingen van medewerkers over de zwakke beveiliging, bleef het bedrijf publieke verklaringen afleggen waarin werd gesteld dat de cybersecurity op orde was.

De rechter had vorig jaar al aangegeven dat er geen sprake was van misleiding, aangezien de wet geen gedetailleerde risicowaar-schuwingen vereiste. Toch erkende de rechter dat de beveiliging van SolarWinds niet voldeed aan de basis-normen. De zaak wordt nu beëindigd, maar de gevolgen van het incident blijven voor veel bedrijven een waarschuwing over de gevaren van onvoldoende beveiliging van kritieke systemen.

Meta-directie schikt Cambridge Analytica zaak voor 190 miljoen dollar

Mark Zuckerberg en meerdere directieleden van Meta hebben ingestemd met een schikking van 190 miljoen dollar in een rechtszaak die was aangespannen door aandeelhouders naar aanleiding van het Cambridge Analytica schandaal. De

aandeelhouders stelden dat zij onvolledig waren geïnformeerd over de risico's die gepaard gingen met het verzamelen en mogelijk misbruiken van gebruikersgegevens via de Facebook app This is your digital life. Volgens de claim had Cambridge Analytica toegang verkregen tot gegevens van in totaal 87 miljoen gebruikers zonder hun toestemming. De eisers voerden aan dat de directie de impact hiervan kende, maar dit niet adequaat communiceerde.

Daarnaast werd gesteld dat de eerdere schikking van 5 miljard dollar tussen Meta en de Amerikaanse toezichthouder FTC was ingegeven door de intentie om Zuckerberg persoonlijk te beschermen tegen mogelijke financiële gevolgen. Door bewust een hoger bedrag te accepteren zou zijn voorkomen dat hij een deel van de boete zelf zou moeten betalen. Het huidige schikkingsbedrag zal worden betaald door Meta en gaat niet naar individuele investeerders, maar wordt intern verwerkt. De voorgestelde regeling moet nog worden goedgekeurd door de rechter. Het vermogen van Zuckerberg wordt door bronnen geschat op meer dan 200 miljard dollar.

Ontslagen IT'er reset uit wraak duizenden wachtwoorden van ex-collega's

Een 35-jarige man uit de Verenigde Staten heeft zich schuldig verklaard aan het resetten van duizenden wachtwoorden van ex-collega's na zijn ontslag bij een Amerikaans afvalverwerkingsbedrijf. De man, die als IT-contractor werkte, kreeg na zijn ontslag nog toegang tot het bedrijfsnetwerk door zich voor te doen als een andere contractor. Hij gebruikte een PowerShell-script om maar liefst 2500 wachtwoorden te resetten, wat leidde tot een massale uitlogactie voor medewerkers in meerdere staten.

Het incident veroorzaakte meer dan 862.000 dollar schade aan het bedrijf, met herstelkosten, verlies van productiviteit en verstoring van klantendiensten. De verdachte probeerde zijn sporen te wissen door systeemlogs te verwijderen, maar zijn acties werden uiteindelijk opgemerkt. Deze zaak benadrukt de noodzaak voor bedrijven om strikte toegangscontrole en accountbeheermaatregelen te treffen bij het beëindigen van dienstverbanden. Het is essentieel dat systemen worden beschermd tegen dergelijke aanvallen, waarbij kwaadwillende actoren misbruik maken van verouderde toegang.

De man kan een gevangenisstraf van maximaal tien jaar en een boete van 250.000 dollar krijgen. De rechter zal op 30 januari 2026 uitspraak doen.

VS schrapt cyberbeveiligingseisen na Chinese hack op telecomnetwerken

De Amerikaanse Federal Communications Commission (FCC) heeft recentelijk besloten verschillende cybersecuritymaatregelen voor telecombedrijven in te trekken. Deze maatregelen waren oorspronkelijk ingevoerd na de onthulling van een grootschalige hack door de Chinese hackercollectief Salt Typhoon. Het doel van de regels was om telecomproviders te dwingen strengere beveiligingsmaatregelen te nemen, met als focus het beschermen van netwerken die door de overheid voor afluisterdoeleinden worden gebruikt. De strengere eisen omvatten onder andere de verplichting voor telecombedrijven om jaarlijkse certificaten in te leveren en risicomanagementplannen op te stellen.

Volgens de FCC waren deze regels echter ineffectief en te vaag, en hadden ze geen wezenlijke impact op het oplossen van de cyberbeveiligingsproblemen. De FCC stelde dat de regels een onredelijke financiële last vormden voor de providers zonder dat ze daadwerkelijk bijdroegen aan het verbeteren van de veiligheid van de netwerken. In plaats van het implementeren van strikte en brede regelgeving, wil de toezichthouder nu samenwerken met de telecomindustrie om de cybersecurityaanpak meer op maat en flexibeler te maken.

De beslissing volgt op een incident in 2024, waarbij Salt Typhoon maandenlang toegang had tot netwerken van grote Amerikaanse telecombedrijven, zoals AT&T en Verizon. Dit werd mogelijk doordat de wetgeving op dat moment geen concrete eisen stelde aan de beveiliging van deze netwerken, ondanks dat ze werden gebruikt voor het naleven van afluisterbevoegdheden van de federale overheid. De terugtrekking van de regels werd door velen gezien als een politiek gemotiveerde zet, vooral omdat de maatregelen waren ingesteld tijdens de regering-Biden, waarvan nu de beleidskeuzes worden herzien.

Dit besluit heeft niet alleen invloed op de telecomsector in de VS, maar kan ook bredere implicaties hebben voor de internationale aanpak van cyberdreigingen, vooral in verband met staatsgesponsorde hackgroepen zoals Salt Typhoon. De toekomst van de Amerikaanse cybersecuritywetgeving voor telecombedrijven blijft dus onzeker.