Cybercrimeinfo - cyberdreigingsanalyse (Openbare versie)

15-10-2025:

Omrin herstelt na ransomware-aanval, winkels gedeeltelijk open

Omrin ondervindt momenteel een technische storing als gevolg van een ransomware-aanval. De organisatie werkt hard aan een oplossing, waarbij de kerntaken zoals de inzameling en verwerking van afval ongewijzigd doorgaan. De klantenservice was tijdelijk niet bereikbaar, maar is sinds 14 oktober weer telefonisch bereikbaar via het nummer 0900-2100215. De Estafette Recyclewinkels in Leeuwarden en Harlingen zijn geleidelijk heropend, waarbij in sommige gevallen alleen contante betalingen mogelijk zijn. In Sneek is de winkel vanaf 14 oktober weer open, inclusief pinbetalingen. Verder worden bestaande afspraken voor het ophalen van grofvuil zoveel mogelijk nagekomen. Het liveblog wordt regelmatig geüpdatet met de laatste informatie over de situatie en de herstelmaatregelen.

RIVM haalt website offline na hack via webformulier

Het Rijksinstituut voor Volksgezondheid en Milieu (RIVM) heeft zijn website tijdelijk offline gehaald na een hack. Aanvallers maakten gebruik van een kwetsbaarheid in het webformulier van de site om toegang te krijgen tot de systemen van de organisatie. Hierdoor verschenen er verschillende artikelen met desinformatie, zoals informatie over het zogenaamde "dawn phenomenon" en bloedsuikerspiegelstijgingen in de ochtend. Na de ontdekking van de hack door GeenStijl bevestigde het RIVM dat de site werd afgesloten om het probleem te verhelpen en de kwetsbaarheid te dichten. De technische afdeling van het RIVM is bezig met het controleren van de plug-ins en het herstellen van de site. Het is op dit moment niet bekend wanneer de website weer toegankelijk zal zijn.

Update: Website RIVM weer online na verhelpen van kwetsbaarheid in webformulier

De website van het Rijksinstituut voor Volksgezondheid en Milieu (RIVM) is hersteld nadat deze tijdelijk offline werd gehaald vanwege een kwetsbaarheid in een webformulier. Deze kwetsbaarheid stelde onbevoegden in staat om malafide berichten te plaatsen die naar nepsites verwezen. Het RIVM benadrukte dat er geen toegang tot gevoelige data is geweest en er geen gegevens zijn gelekt. Het probleem is inmiddels opgelost en de malafide berichten zijn verwijderd. De website is weer

volledig toegankelijk, al functioneren de webformulieren nog niet optimaal. Het RIVM werkt aan een snelle oplossing voor dit laatste probleem.

Hacktivisme in 2025: wat hashtags onthullen over digitale campagnes

In 2025 is hacktivisme een wereldwijde dreiging die zowel de surface web als het dark web beïnvloedt. Onderzoek naar meer dan 11.000 berichten van meer dan 120 hacktivistische groepen toont aan dat hun operaties vaak openbaar worden gecoördineerd, vooral via platforms zoals Telegram en X (voorheen Twitter). Hashtags spelen een cruciale rol in de campagnes van hacktivisten, dienen als politieke leuzen, coördineren aanvallen en claimen verantwoordelijkheid voor acties. In 2025 werden 2063 unieke hashtags geïdentificeerd, waarvan de meeste kortstondig waren. DDoS-aanvallen bleken de meest voorkomende cyberaanvallen. De timing van dreigementen, vaak met korte-termijnacties, maakt open-channeldetectie nuttig voor vroege waarschuwingen. Bedrijven moeten prioriteit geven aan DDoS-mitigatie, voortdurende monitoring en snel reageren op bedreigingen die via deze openbare kanalen circuleren.

Russische cybercriminelen verschuiven van RDP-toegang naar het verhandelen van malware-stealer logs

In de Russische cybercriminaliteit is een belangrijke verschuiving gaande. Marktplaatsen en cybercriminelen stappen over van het verkopen van gecompromitteerde RDP-toegang naar het verhandelen van malware-stealer logs. Deze verandering in tactieken heeft wereldwijd impact, aangezien deze logs belangrijke gegevens bevatten, zoals opgeslagen wachtwoorden, cookies, crypto-walletdetails en sessietokens. Stealer malware zoals RedLine, Raccoon en Vidar heeft deze trend versterkt, waarbij aanvallers steeds meer gebruikmaken van deze logs om toegang te krijgen tot systemen en accounts, vaak met grotere stealth en efficiëntie dan traditionele methoden. Deze logs worden snel verhandeld op forums, waarbij aanvallers direct in staat zijn om slachtoffers te imiteren en accounts over te nemen, wat de risico's voor gegevensdiefstal vergroot.
Cyberbeveiligingsprofessionals moeten zich aanpassen door real-time logmonitoring en versnelde incidentrespons in te zetten om deze geautomatiseerde dreigingen te bestrijden.

Chinese hackers misbruiken ArcGIS geo-mapping tool voor langdurige infiltratie

Chinese staats-hackers hebben meer dan een jaar lang onopgemerkt toegang gehad tot een doelwit door een component van de ArcGIS geo-mapping tool om te vormen tot een webshell. Ze gebruikten geldige beheerdersreferenties om in te loggen op een publieke ArcGIS-server die verbonden was met een interne server. Via deze toegang uploadden ze een kwaadaardige Java SOE, die als webshell fungeerde en commando's uitvoerde zonder detectie. De hackers gebruikten de webshell om SoftEther VPN Bridge te installeren, wat een beveiligde verbinding opbouwde naar hun server, waardoor ze verder konden opereren in het netwerk. Deze VPN bleef actief, zelfs als de webshell verwijderd werd. Het aanvallende Flax Typhoon-groep heeft eerder bekendheid verworven door spionagecampagnes en heeft tactieken gebruikt om langdurige toegang tot netwerken te verkrijgen. Esri, de ontwikkelaar van ArcGIS, heeft bevestigd dat dit de eerste keer is dat een SOE op deze manier is misbruikt.

Nieuwe kwetsbaarheid in Android maakt Pixnapping mogelijk voor diefstal van 2FA-codes

Een nieuwe kwetsbaarheid in Android-apparaten, aangeduid als Pixnapping, maakt het mogelijk voor kwaadwillende apps om 2FA-codes en andere gevoelige gegevens zonder toestemming te stelen. Deze kwetsbaarheid maakt gebruik van een side-channel-aanval die gegevens pixel voor pixel kan stelen, zelfs uit apps zoals Google Authenticator. Onderzoekers van onder andere de Universiteit van Californië hebben ontdekt dat de aanval via Android API's werkt, waarbij de app pixels in de renderingspipeline forceert en deze gegevens steelt met behulp van grafische bewerkingen. De aanval kan binnen 30 seconden 2FA-codes verkrijgen. Het probleem treft apparaten van Google en Samsung met Android 13 tot 16. Hoewel Google een patch heeft uitgebracht, is er een workaround die de aanval opnieuw mogelijk maakt. De kwetsbaarheid is geclassificeerd onder CVE-2025-48561, met een CVSS-score van 5,5.

Axis Communications kwetsbaarheid onthult Azure-opslagaccountreferenties

Een ernstige kwetsbaarheid in de Autodesk Revit-plugin van Axis Communications heeft Azure-opslagaccountreferenties blootgelegd, wat aanzienlijke beveiligingsrisico's veroorzaakt voor klanten en potentiële kettaanvallen binnen de

architectuur- en ingenieurssector mogelijk maakt. De kwetsbaarheid werd ontdekt in juli 2024 toen Azure Shared Access Signature (SAS)-tokens in een digitaal ondertekend DLL-bestand, "AzureBlobRestAPI.dll", werden aangetroffen. Deze tokens boden ongeautoriseerde lees- en schrijfrechten voor drie Azure-opslagaccounts van Axis Communications. Deze accounts bevatten essentiële bestanden zoals MSI-installateurs en Revit Family Architecture-bestanden die door klanten worden gebruikt voor bouwinformatieprojecten. De ontdekking leidde tot een langdurig herstelproces en het patchen van de kwetsbaarheid. Hoewel aanvankelijk een poging werd gedaan om de beveiliging te verbeteren door code te obfusceren, bleken de referenties alsnog toegankelijk, waardoor de aanvallers eerder aangebrachte herstelmaatregelen konden omzeilen. Axis Communications heeft de kwetsbaarheden inmiddels volledig gepatcht.

Elastic Cloud Enterprise kwetsbaarheid stelt aanvallers in staat om schadelijke commando's uit te voeren

Elastic heeft een kritieke kwetsbaarheid bekendgemaakt in zijn Elastic Cloud Enterprise (ECE)-platform. Deze kwetsbaarheid maakt het mogelijk voor beheerders met kwaadwillige bedoelingen om willekeurige commando's uit te voeren en gevoelige gegevens te exfiltreren. Het probleem, aangeduid als CVE-2025-37729, heeft te maken met een onjuiste neutralisatie van speciale elementen in de Jinjava-template-engine. Aangevallen versies van ECE kunnen leiden tot code-executie via kwaadwillig ingevoerde payloads in de beheerdersconsole. Deze kwetsbaarheid treft ECE-versies van 2.5.0 tot en met 3.8.1 en 4.0.0 tot 4.0.1. Elastic raadt aan om te upgraden naar gepatchte versies (3.8.2 of 4.0.2). Bedrijven kunnen hun risico verminderen door toegang tot de beheerdersconsole strikt te controleren en verdachte activiteiten in logbestanden te monitoren.

Risico op Secure Boot-bypass bedreigt bijna 200.000 Linux-laptops van Framework

Ongeveer 200.000 laptops van het Amerikaanse bedrijf Framework, die draaien op Linux, bevatten een kwetsbaarheid die kan worden misbruikt om de Secure Boot-bescherming te omzeilen. Deze kwetsbaarheid komt door een ondertekende UEFI-shellcomponent die een 'memory modify' (mm) commando bevat. Dit commando geeft directe toegang tot het systeemgeheugen en kan worden misbruikt om de verificatie van handtekeningen van UEFI-modules uit te schakelen. Dit maakt het

mogelijk voor aanvallers om malware zoals bootkits in het systeem te laden, die moeilijk te detecteren zijn en blijven na herinstallatie van het besturingssysteem. Framework heeft aangekondigd de kwetsbaarheid aan te pakken met beveiligingsupdates, maar voor systemen die nog geen patch hebben, wordt aanbevolen om fysieke toegang te blokkeren of het DB-sleutel te verwijderen via de BIOS.

Analyse van PolarEdge backdoor in QNAP-apparaten

De PolarEdge backdoor, ontdekt in 2025, maakt gebruik van de kwetsbaarheid CVE-2023-20118 in QNAP-apparaten om een TLS-gebaseerde backdoor in te voeren. Dit implantaat stelt aanvallers in staat om op afstand commando's uit te voeren via een C2-server. De backdoor verzamelt dagelijks vingerafdrukken van de getroffen systemen en kan meerdere modi ondersteunen, zoals een servermodus, een connect-back modus en een debugmodus. Het implantaat is ontworpen om anti-analysetechnieken toe te passen, zoals het verbergen van processen en het gebruik van encryptie om zijn configuratie te beveiligen. De techniek omvat onder andere het gebruik van XOR-encryptie en de PRESENT-blockcipher voor het beveiligen van gedeeltes van de backdoor. Het doel van de PolarEdge backdoor is waarschijnlijk om andere kwetsbaarheden in apparaten van verschillende merken te exploiteren, waarbij ook QNAP, Asus en Synology routers doelwitten zijn.

ClearFake JavaScript-payload geleverd via gecompromitteerd domein

Een domein dat geassocieerd wordt met de ClearFake malwarecampagne is geïdentificeerd. Het domein toont momenteel een Cloudflare-phishingwaarschuwing en is gemeld voor kwaadaardige activiteiten. ClearFake-campagnes zijn bekend om het verspreiden van schadelijke scripts die payloads afleveren of gebruikers doorsturen naar phishingpagina’s. Het domein in kwestie is e1mx.fkur8[.]ru, en het wordt beschouwd als een betrouwbare indicator van schadelijke activiteit met een vertrouwensniveau van 100%. Verdere onderzoeken tonen aan dat het domein gebruikt wordt voor het leveren van JavaScript-payloads die zich voordoen als beveiligings- of software-updatewaarschuwingen. Verdere actie wordt aanbevolen, waaronder het blokkeren van dit domein en de bijbehorende IP-adressen, evenals het monitoren van sessies die gebruikers naar valse browser-updatepagina’s leiden.

Onderzoekers onthullen aanvalsketen en mogelijkheden van MonsterV2-malware van TA585

Cyberbeveiligingsonderzoekers hebben een nieuwe dreigingsactor, TA585, geïdentificeerd, die de MonsterV2-malware verspreidt via phishingcampagnes. De malware, een remote access trojan (RAT) en stealer, werd in februari 2025 voor het eerst op criminelenforums geadverteerd. TA585 heeft zijn eigen infrastructuur en malware-installatietechnieken ontwikkeld, wat het onderscheiden maakt van andere cybercriminelen. De malware wordt voornamelijk verspreid via phishingberichten die zich voordoen als berichten van de Amerikaanse belastingdienst (IRS), die gebruikers naar schadelijke websites leiden. Na de infectie kan MonsterV2 gegevens stelen, cryptocurrency-adressen vervangen, en op afstand systemen besturen. De malware is geprijsd op $800 per maand voor de standaardversie, en $2.000 voor de Enterprise-versie. Verder maakt het gebruik van geavanceerde technieken zoals anti-debugging en privilege-escalatie om detectie te vermijden.

AI-geassisteerde malvertising: hoe chatbots worden gebruikt om oplichtingsscams te verspreiden

Cybercriminelen maken misbruik van AI-chatbots, zoals Grok van X (voorheen Twitter), om phishing-scamlinks te verspreiden. Deze techniek, genaamd "Grokking," houdt in dat kwaadwillenden een video met clickbait plaatsen en de AI-chatbot vragen naar de herkomst van de video. De chatbot, die vaak als vertrouwde bron wordt gezien, versterkt de schadelijke link door deze in zijn antwoord op te nemen. Deze video's bereiken miljoenen gebruikers, wat de verspreiding van malware en diefstal van inloggegevens vergemakkelijkt. Het probleem van dergelijke aanvallen wordt verergerd door het gebruik van "prompt injectie," waarbij aanvallers schadelijke instructies aan de AI geven. Dit onderstreept de risico's van blind vertrouwen op AI-uitvoer, vooral bij openbare bots die gegevens verwerken die mogelijk "geïnfecteerd" zijn met kwaadaardige inhoud.

Hackers vallen macOS-gebruikers aan met vervalste Homebrew-websites om schadelijke payloads in te voegen

Een geavanceerde aanval richt zich op macOS-gebruikers via vervalste Homebrew-installatiewebsites die schadelijke payloads leveren naast legitieme pakketbeheer-installaties. De aanvallers maken pixel-perfecte replicaties van de officiële

Homebrew-installatiepagina's en gebruiken geavanceerde technieken om de klembord van de gebruiker te manipuleren. De frauduleuze websites, zoals homebrewfaq[.]org en homebrewclubs[.]org, dwingen gebruikers om de kopieerknop te gebruiken, waarmee schadelijke commando's in hun klembord worden ingevoegd. Deze commando's worden uitgevoerd samen met de legitieme installatiecommando's, waardoor malware onopgemerkt kan worden geïnstalleerd. Dit vormt een nieuwe benadering van supply chain-aanvallen, waarbij de aanvallers niet de pakketrepositories zelf compromitteren, maar het installatieproces aanvallen. De aanvallers gebruiken JavaScript om hun payloads in te voegen, wat de kans op detectie verkleint.

Agressieve misbruik van ScreenConnect voor ongevraagde toegang tot systemen

Cybercriminelen maken steeds vaker misbruik van de software ConnectWise ScreenConnect, een remote monitoring en management (RMM) tool, om ongemerkt toegang te krijgen tot systemen. Dit gebeurt via geavanceerde phishingcampagnes die slachtoffers misleiden met valse IT-waarschuwingen. De aanvallers gebruiken aangepaste installerbestanden om ScreenConnect te implementeren, waardoor traditionele beveiligingssystemen moeilijkheden ondervinden bij het detecteren van de aanval. Na installatie creëert de malware een verborgen Windows-service die aanvallers volledige toegang geeft tot bestandssystemen en netwerken. De aanvallers maken gebruik van op maat gemaakte configuraties en encryptie om hun sporen te verbergen, wat het voor beveiligingsteams moeilijk maakt om de activiteit te traceren en te stoppen. Door deze techniek blijft de aanval moeilijk detecteerbaar, wat de ernst van het gevaar vergroot.

De opkomst van autonome AI-agents en de nieuwe beveiligingsrisico's

Autonome AI-agents zijn niet langer slechts hulpmiddelen die taken uitvoeren, maar nemen zelf acties zoals het openen van tickets, analyseren van logboeken en het oplossen van incidenten. Deze AI-agents maken beslissingen sneller dan mensen kunnen volgen, wat nieuwe beveiligingsrisico's introduceert. Ze kunnen zelfstandig werken zonder menselijke tussenkomst, wat hen krachtig maakt, maar ook gevaarlijk. Bedrijven implementeren steeds vaker deze agents, maar zonder voldoende zichtbaarheid of controles, wat leidt tot "shadow AI". Dit maakt het moeilijk om acties terug te traceren naar de oorspronkelijke gebruiker. Het is belangrijk dat

bedrijven nieuwe regels invoeren voor het beheren van AI-agents, zoals het bijhouden van hun levenscyclus en het toepassen van context op hun acties. Het doel is niet om AI-agents te stoppen, maar om effectieve beveiligingsmaatregelen en governance te implementeren om ongecontroleerde processen te voorkomen.

Hackers doen zich voor als openai en sora om inloggegevens te stelen

Een phishingcampagne richt zich de laatste weken op bedrijfs- en consumentenaccounts door zich voor te doen als de inlogportalen van OpenAI en Sora. De aanvallers versturen e-mails die als legitieme meldingen lijken, waarin ze ontvangers waarschuwen voor een accountschorsing of verdachte activiteiten. De berichten bevatten links naar vervalste inlogpagina's die sterk lijken op de originele sites, inclusief SSL-certificaten. Onderzoekers van Unit 42 ontdekten dat de aanvallers gebruikmaken van een meerfasenloader, geschreven in obfuscating JavaScript, die na het invullen van de inloggegevens kwaadaardige payloads in de browser injecteert. De ingediende gegevens worden vervolgens naar een command-and-controlserver gestuurd, terwijl de gebruikers doorgestuurd worden naar de legitieme site, waardoor de inbraak moeilijker te detecteren is. Deze aanvalsmethode stelt de aanvallers in staat om inloggegevens te verzamelen voor zowel persoonlijke als zakelijke accounts zonder opgemerkt te worden.

Britse overheid meldt recordaantal cyberaanvallen met nationale impact

Het Verenigd Koninkrijk heeft het afgelopen jaar een recordaantal cyberaanvallen ervaren die nationale gevolgen hadden. Tussen september van het vorige jaar en augustus dit jaar werden 204 cyberaanvallen geregistreerd, vergeleken met 89 in het jaar ervoor. Het National Cyber Security Centre (NCSC) meldt dat in totaal 429 incidenten zijn afgehandeld, waarvan 18 als zeer significant werden gekarakteriseerd, met het potentieel om essentiële diensten te verstoren. Bekende Britse bedrijven zoals Jaguar Land Rover, Marks & Spencer, en Transport for London waren slachtoffers van deze aanvallen. De toename in aanvallen wordt toegeschreven aan een kleine groep actoren die misbruik maken van kwetsbaarheden in onder andere Microsoft SharePoint Server en Ivanti Connect Secure. Het NCSC benadrukt dat cyberbeveiliging niet alleen een technische verantwoordelijkheid is, maar dat bestuurders van organisaties ook moeten bijdragen aan de cyberweerbaarheid.

Australische overheid roept bedrijven op om legacy IT te vervangen

De Australische overheid waarschuwt bedrijven voor de risico's van verouderde IT-systemen, nu Microsoft de ondersteuning voor Windows 10 beëindigt. Het Australische Cyber Security Centre (ACSC) benadrukt dat legacy IT een belangrijke kwetsbaarheid vormt, aangezien dergelijke systemen vaak niet langer worden ondersteund door leveranciers. Dit vergroot het risico op cyberincidenten en maakt het moeilijker om deze systemen effectief te beveiligen. De overheid adviseert bedrijven om legacy IT te vervangen door systemen die nog wel worden ondersteund. Indien vervanging niet mogelijk is, moeten tijdelijke maatregelen worden genomen. Het ACSC raadt verder aan om risico’s van derde partijen te beheersen, logging te implementeren, en zich voor te bereiden op post-quantum cryptografie. Dit advies komt na een jaar waarin het ACSC vaker betrokken was bij cyberincidenten en waarschuwingen gaf voor malafide activiteiten.

Windows 10 blijft populair ondanks naderende einde ondersteuning

Volgens onderzoek van TeamViewer draait wereldwijd nog altijd meer dan veertig procent van de computers op Windows 10. Dit is opvallend gezien Microsoft vanavond de officiële ondersteuning voor dit besturingssysteem beëindigt. TeamViewer baseerde zijn bevindingen op 250 miljoen geanonimiseerde sessies tussen juli en september 2025, waaruit bleek dat 41 procent van de apparaten op Windows 10 draait, terwijl Windows 11 47 procent van de systemen vertegenwoordigt. Kaspersky meldde dat zelfs 53 procent van hun gebruikers nog op Windows 10 werkt, vooral in zakelijke omgevingen. In Nederland ligt het gebruik van Windows 10 op bijna 39 procent van de computers. Microsoft biedt Europese gebruikers met een Microsoft-account de mogelijkheid om nog een jaar gratis updates te ontvangen, terwijl bedrijven tegen betaling drie extra jaren beveiligingsupdates kunnen verkrijgen.