Cybercrimeinfo - cyberdreigingsanalyse (Openbare versie)

10-10-2025:

Zuid-Hollandse onderwijsgroep lekt honderden e-mailadressen door phishingaanval

De Willem van Oranje Onderwijsgroep in Gorinchem is slachtoffer geworden van een phishingaanval, waarbij honderden e-mailadressen zijn gelekt. Medewerkers trapten in een phishingmail met een Office 365-link, waardoor aanvallers toegang kregen tot 2FA-beveiligde e-mailaccounts. Na het inloggen met twee-factor-authenticatie kreeg de hacker tijdelijk controle over de accounts, maar het beveiligingssysteem blokkeerde de toegang na een uur. Echter, na de voorjaarsvakantie werden de accounts per ongeluk weer geactiveerd. Een andere organisatie waar de onderwijsgroep mee samenwerkt, werd eveneens getroffen, wat leidde tot een kettingreactie waarbij vijf medewerkers opnieuw op phishinglinks klikten. Uiteindelijk konden 450 e-mailadressen worden buitgemaakt. Na ontdekking werd het incident gerapporteerd bij de Autoriteit Persoonsgegevens en werden wachtwoorden van alle medewerkers gereset.

Rusland maakt gebruik van AI in cyberaanvallen op Oekraïne

Russische hackers hebben kunstmatige intelligentie (AI) ingezet in hun cyberaanvallen op Oekraïne, met een significant stijgende trend in 2025. In de eerste helft van 2025 werden 3.018 cyberincidenten geregistreerd, een toename ten opzichte van het tweede halfjaar van 2024. De aanvallen richten zich niet alleen op phishing, maar ook op geavanceerde malware die waarschijnlijk met AI is gegenereerd. Bekende aanvallers, zoals UAC-0219 en UAC-0226, verspreiden kwaadaardige software via phishingcampagnes gericht op de Oekraïense defensie en kritieke infrastructuur. Daarnaast werden kwetsbaarheden in populaire webmailsoftware zoals Roundcube en Zimbra misbruikt voor zero-click-aanvallen, waarmee aanvallers toegang kregen tot gevoelige gegevens. De inzet van legitieme online diensten, zoals Google Drive en Telegram, voor het hosten van malware, is een groeiende trend. Deze aanvallen zijn onderdeel van een bredere hybride oorlogsvoering waarbij cyberaanvallen en fysieke militaire operaties worden gecombineerd.

Ursula von der Leyen waarschuwt voor Russische hybride oorlog

Ursula von der Leyen, voorzitter van de Europese Commissie, waarschuwde in een toespraak voor de toenemende dreiging van Russische cyberaanvallen en saboteurs als onderdeel van een hybride oorlog tegen Europa. Ze noemde recente incidenten, zoals schendingen van het Estse luchtruim en drones in verschillende EU-landen, als onderdeel van een zorgwekkend patroon van dreigingen. Von der Leyen benadrukte dat deze aanvallen geen toevalligheden zijn, maar deel uitmaken van een gecoördineerde campagne om de EU te destabiliseren. Ze drong aan op een gezamenlijke Europese strategie om snel te reageren op dergelijke dreigingen. In haar speech benadrukte ze de noodzaak van een nieuwe mindset en het ontwikkelen van strategische capaciteiten, in nauwe samenwerking met NAVO, om Europa tegen deze hybride oorlog te beschermen.

APT35 van IRGC onthult: structuur, tools en spionage-operaties

APT35, een aan de Iraanse Revolutionaire Garde (IRGC) gelinkt hackercollectief, heeft zijn aanvallen sinds de jaren 2010 voortdurend aangepast. Aanvankelijk gericht op phishing-campagnes voor het verzamelen van inloggegevens, heeft de groep nu een geavanceerd toolkit ontwikkeld voor netwerkdoorbraak en langdurige spionage. De aanvallen beginnen met zorgvuldig samengestelde spear-phishing berichten, die kwetsbaarheden in Office-macro's misbruiken om achterdeurtjes te installeren. De gebruikte toolset bevat zowel op maat gemaakte als publieke componenten, waarmee de onderzoekers unieke codevingerafdrukken kunnen volgen, zelfs bij veranderingen in payloads. De groep maakt gebruik van .NET-gebaseerde implantaten en technieken zoals in-memory uitvoering om forensisch onderzoek te bemoeilijken. Gecompromitteerde netwerken hebben te maken gehad met gegevensdiefstal, waaronder diplomatieke communicatie en strategische informatie. APT35 gebruikt open-source intelligence (OSINT) voor het maken van overtuigende lures en blijft via versleutelde kanalen onopgemerkt opereren.

Russische hacktivisten richten zich op kritieke infrastructuur met aanval op nepwaterzuiveringsinstallatie

Een Russische hacktivistengroep, TwoNet, heeft zich in minder dan een jaar tijd van DDoS-aanvallen naar aanvallen op kritieke infrastructuur verplaatst. Recent claimden ze een aanval op een waterzuiveringsinstallatie, maar deze bleek een honeypot, opgezet door onderzoekers om aanvallers te monitoren. De aanval, die in september

plaatsvond, onthulde dat TwoNet binnen 26 uur van initiële toegang overging tot verstorende acties. De hackers wisten toegang te krijgen via standaardwachtwoorden, en gebruikten een oude kwetsbaarheid om meldingen op de HMI (Human Machine Interface) te triggeren, met als boodschap "Hacked by Barlati". Ze verstoorden processen door real-time updates uit te schakelen en wijzigingen aan te brengen in de PLC-instellingen. Forescout, het onderzoeksbedrijf dat de aanval volgde, waarschuwt kritieke infrastructuurorganisaties voor zwakke authenticatie en blootstelling aan het openbare internet.

GitLab publiceert kritieke beveiligingsupdates voor meerdere kwetsbaarheden die DoS-aanvallen mogelijk maken

GitLab heeft belangrijke beveiligingsupdates vrijgegeven voor zowel de Community Edition (CE) als de Enterprise Edition (EE). De nieuwe versies, 18.4.2, 18.3.4 en 18.2.8, lossen meerdere kwetsbaarheden op die kunnen leiden tot denial-of-service (DoS)-aanvallen en ongeautoriseerde toegang. De kwetsbaarheden, waaronder een autorisatie-bypass in GraphQL, kunnen ernstige verstoringen veroorzaken in zelf-beheerde GitLab-installaties. Gebruikers van GitLab.com en GitLab Dedicated zijn al beschermd door deze patches. GitLab roept gebruikers van zelf-beheerde installaties op om de updates onmiddellijk door te voeren om systeemuitval en gegevensmanipulatie te voorkomen. De kwetsbaarheden betreffen zowel geauthenticeerde als niet-geauthenticeerde gebruikers en kunnen aanzienlijke risico's voor code repositories en ontwikkelingspijplijnen veroorzaken. GitLab benadrukt het belang van proactieve updates om de beveiliging te waarborgen.

Linux Kernel ksmbd-bestandssysteem kwetsbaarheid uitgebuit – PoC vrijgegeven

Onderzoekers hebben een volledig proof-of-concept (PoC) exploit vrijgegeven voor een ernstige kwetsbaarheid in de Linux kernel's ksmbd-module. Deze kwetsbaarheid, aangeduid als CVE-2025-37947, betreft een out-of-bounds schrijf-fout die door een geauthenticeerde lokale aanvaller kan worden misbruikt om root-toegang te verkrijgen op een kwetsbaar systeem. De kwetsbaarheid doet zich voor in de ksmbd_vfs_stream_write() functie en wordt veroorzaakt door onjuiste groottevalidatie bij het verwerken van gegevens. Door deze fout kunnen aanvallers geheugen overschrijven en gebruik maken van een "use-after-free" voor het verkrijgen van root-rechten. Het PoC-exploit is inmiddels openbaar gemaakt, waarmee andere

beveiligingsprofessionals de impact kunnen beoordelen. Ondanks dat de exploit momenteel alleen voor lokale toegang werkt, kan remote exploitatie moeilijker zijn zonder aanvullende kwetsbaarheden. Beheerders wordt geadviseerd hun systemen te patchen zodra updates beschikbaar komen.

PoC-exploit voor code-executie kwetsbaarheid in Nothing Phone

Er is een proof-of-concept (PoC) exploit vrijgegeven voor een kritieke kwetsbaarheid in de secure boot chain van de Nothing Phone (2a) en CMF Phone 1, die mogelijk ook andere apparaten met MediaTek-systemen aantast. De kwetsbaarheid, ontdekt door onderzoeker R0rt1z2, stelt aanvallers in staat om willekeurige code uit te voeren met de hoogste privileges, wat de secure boot-procedure verstoort. Dit probleem ontstaat door een logische fout in de MediaTek boot chain, waarbij een belangrijk component niet goed wordt gecontroleerd wanneer de bootloader ontgrendeld is. De exploit maakt gebruik van een fout in de Preloader fase, waardoor ongecontroleerde code kan worden geladen voordat het besturingssysteem wordt opgestart. De kwetsbaarheid is bevestigd in de Nothing Phone (2a) en CMF Phone 1, en mogelijk ook aanwezig in andere MediaTek-apparaten. Gebruikers worden gewaarschuwd voor de risico's bij het uitvoeren van de exploit.

Kritieke kwetsbaarheid (CVE-2025-36636) ontdekt in Tenable Security Center, patch onmiddellijk nodig

Er is een kritieke kwetsbaarheid (CVE-2025-36636) ontdekt in Tenable Security Center, een veelgebruikte platform voor kwetsbaarheidsbeheer. Deze kwetsbaarheid, met een CVSS-score van 10.0, stelt een aanvaller in staat om ongeautoriseerde toegang te krijgen tot gevoelige gebieden binnen het platform. Dit kan leiden tot ernstige gevolgen voor de vertrouwelijkheid, integriteit en beschikbaarheid van het systeem. De kwetsbaarheid is te wijten aan onjuiste toegangscontrole, waardoor een geauthenticeerde gebruiker toegang kan krijgen tot gebieden buiten hun bevoegdheden. Het wordt sterk aanbevolen om over te schakelen naar Tenable Security Center versie 6.7.0 of hoger om de kwetsbaarheid te verhelpen. Organisaties moeten hun monitoringcapaciteiten uitbreiden en verdachte activiteiten snel detecteren om mogelijke inbraken te identificeren en adequaat te reageren.

SonicWall klantendata gestolen door aanvallers via cloudback-up

SonicWall heeft bevestigd dat aanvallers de firewall-configuratie van alle klanten die gebruikmaken van de cloudback-updienst hebben gestolen. De gestolen bestanden bevatten versleutelde inloggegevens en configuratie-informatie die cybercriminelen kunnen helpen bij gerichte aanvallen. Eerder werd gemeld dat minder dan vijf procent van de klanten getroffen was, maar recentere informatie toont aan dat alle klanten met cloudback-up kwetsbaar zijn geworden. SonicWall heeft het incident omschreven als een "cloud backup security incident" en heeft de vorige verwijzingen naar bruteforce-aanvallen verwijderd. Klanten worden aangemoedigd om in te loggen op de MySonicWall portal om te controleren of hun systemen risico lopen. SonicWall heeft ook aanvullende beveiligingsmaatregelen doorgevoerd, maar de details hierover blijven onbekend.

Crimson Collective richt zich op AWS-cloudomgevingen voor datadiefstal

De dreigingsgroep Crimson Collective heeft de afgelopen weken Amazon Web Services (AWS)-cloudomgevingen aangevallen, waarbij ze toegang kregen tot gevoelige data en bedrijven afpersen. Ze hebben onlangs de verantwoordelijkheid opgeëist voor de aanval op Red Hat, waarbij 570 GB aan gegevens uit duizenden privé GitLab-repositories werden gestolen. Om toegang te krijgen tot AWS, gebruiken de aanvallers onder andere het open-source hulpmiddel TruffleHog om blootgestelde AWS-referenties te vinden. Nadat ze toegang hebben verkregen, creëren ze nieuwe gebruikers en verhogen hun bevoegdheden, waardoor ze volledige controle over de cloudomgevingen krijgen. De aanvallers verzamelen gegevens, modificeren wachtwoorden van databases en exfiltreren deze naar andere opslagdiensten zoals S3. Crimson Collective verstuurt vervolgens afpersingsberichten via e-mail. AWS raadt klanten aan kortdurende, minimaal bevoorrechte referenties te gebruiken en IAM-beperkingen te implementeren om dergelijke aanvallen te voorkomen.

nieuwe FileFix-aanval maakt gebruik van cache-smuggling om beveiligingssoftware te omzeilen

Een nieuwe variant van de FileFix-aanval maakt gebruik van cache-smuggling om op een slachtoffercomputer een kwaadaardige ZIP-bestand te downloaden en beveiligingssoftware te omzeilen. De aanval lijkt afkomstig van een "Fortinet VPN Compliance Checker" en werd ontdekt door cybersecurityonderzoeker

P4nd3m1cb0y. In deze phishing-aanval wordt een nepdialog weergegeven die gebruikers aanzet om een ogenschijnlijk legitiem pad naar een Fortinet-programma in de Windows Verkenner in te voeren. Dit pad bevat echter verborgen PowerShell-opdrachten die schadelijke code activeren. De kwaadaardige bestanden worden verstopt in de cache van Google Chrome en kunnen worden uitgevoerd zonder dat het beveiligingssoftware detecteert. Het gebruik van cache-smuggling zorgt ervoor dat de malware voorbij veel beveiligingsproducten komt. Dit soort aanvallen is snel overgenomen door ransomwaregroepen en andere cybercriminelen.

De Watergroep (B) waarschuwt voor phishing door samenwerking met Farys

De Watergroep in Belgie waarschuwt klanten voor phishing-aanvallen die gebruikmaken van hun aankomende samenwerking met waterleverancier Farys, die op 1 januari 2026 officieel van start gaat onder de naam WaterUnie. Cybercriminelen spelen in op deze verandering door valse e-mails en sms'jes te versturen die lijken te komen van WaterUnie. De Watergroep benadrukt dat klanten niet gevraagd worden om hun gegevens opnieuw door te geven, en dat zij dit zelfstandig kunnen aanpassen via hun klantenzone. Klanten wordt geadviseerd om betalingen via domiciliëring te regelen en verdachte e-mails door te sturen naar De Watergroep, die probeert de afzenders te blokkeren. De samenwerking tussen De Watergroep en Farys heeft als doel een duurzamere waterproductie, maar voor klanten verandert er niets in de dienstverlening.

Mustang Panda gebruikt nieuwe DLL side-loading techniek voor malwaredistributie

De cyberdreigingsactor Mustang Panda heeft recent een nieuwe aanpak geïntroduceerd om malware te verspreiden, door middel van DLL side-loading. De aanval maakt gebruik van phishingmails waarin slachtoffers een ZIP-bestand ontvangen met een bedrieglijk uitvoerbaar bestand, "Voice for the Voiceless Photos.exe", samen met een verborgen DLL-bestand, libjyy.dll. Dit bestand is gemarkeerd met system- en verborgen-attributen, waardoor het moeilijker te detecteren is. Wanneer het bedrieglijke bestand wordt uitgevoerd, laadt het de DLL via LoadLibraryW, wat de malware routine activeert. De techniek maakt het gebruik van dynamische API-resolutie en versleuteling om het gedrag te verbergen en traditionele detectie methoden te omzeilen. Het einddoel is het verkrijgen van persistente toegang tot het systeem en het exfiltreren van gegevens naar een

command-and-control server, waarbij verschillende technieken zoals register sleutels en geplande taken worden gebruikt om de malware actief te houden.

Scattered Lapsus$ Hunters lanceert nieuwe lek-site voor gestolen Salesforce-gegevens

De cybercriminelen van Scattered Lapsus$ Hunters hebben hun afpersingscampagne vergroot door een nieuwe lek-site te lanceren waarop gestolen Salesforce-gegevens worden gedreigd openbaar te maken. Dit collectief, dat bestaat uit de bekende dreigingsactoren ShinyHunters, Scattered Spider en Lapsus$, richt zich op Salesforce, een wereldwijd veelgebruikte CRM-plaatform, door bedrijven met gestolen klantgegevens te bedreigen. De aanvallers gebruikten onder andere social engineering technieken, zoals vishing, om toegang te krijgen tot Salesforce-systemen en exfiltratie van gevoelige data mogelijk te maken. Daarnaast exploitereerden ze OAuth-integratietokens voor blijvende toegang. De nieuwe lek-site bevat claims over de hoeveelheid gestolen data en dreigt met openbaarmaking, tenzij de gevraagde betalingen worden voldaan. De deadline voor betaling is vastgesteld op 10 oktober 2025.

Hackers compromitteren databases met legitieme commando's

Een nieuwe vorm van ransomware-aanvallen maakt gebruik van legitieme databasecommando's om systemen wereldwijd te compromitteren. In plaats van traditionele malware te gebruiken, misbruiken aanvallers blootgestelde databases door standaard databasefunctionaliteit te manipuleren, zoals het stelen, wissen en losgeld eisen van kritieke gegevens. Deze aanvallen richten zich op internet-verbonden databaseservers met zwakke wachtwoorden of geen authenticatie. De aanvallers gebruiken legitieme SQL-commando's om gegevens te extraheren en destructieve bewerkingen uit te voeren, zoals het verwijderen van databases. Deze methode is moeilijk te detecteren omdat er geen schadelijke binaries op het systeem worden geplaatst. De aanvallen maken gebruik van geautomatiseerde bots die constant internet scannen naar misconfiguraties, waardoor organisaties kwetsbaar zijn. Sinds de eerste waarnemingen in 2017 is het aantal gevallen sterk gestegen, waarbij aanvallers snel nieuwe doelen kunnen compromitteren zodra ze online zijn.

FreePBX SQL-injectie kwetsbaarheid gebruikt voor databaseaanpassing

Een ernstige SQL-injectiekwetsbaarheid in FreePBX, een veelgebruikte PBX-systeem voor VoIP-infrastructuur, stelt aanvallers in staat om database-inhoud te manipuleren en willekeurige code uit te voeren. Deze kwetsbaarheid, aangeduid als CVE-2025-57819, maakt misbruik van onbeveiligde webtoepassingsparameters, specifiek gericht op de databasebeheersystemen van FreePBX. Door middel van SQL-injecties via de ajax.php-endpoint kunnen aanvallers kwaadaardige verzoeken versturen die onwettige gegevensinvoegingen in de cron_jobs-databasetabel veroorzaken. Dit creëert persistentie en zorgt voor ongeautoriseerde toegang. Analyse van actieve exploitatiecampagnes toont aan dat de aanvallers geavanceerde technieken gebruiken die verder gaan dan eenvoudige database-aanpassingen, waaronder stealth en zelfvernietigende mechanismen om forensisch onderzoek te bemoeilijken.

hackers misbruiken css-eigenschappen voor verborgen tekstaanvallen

Hackers maken gebruik van een nieuwe techniek, bekend als hidden text salting, om kwaadaardige codes in e-mailberichten te injecteren. Deze techniek maakt gebruik van de eigenschappen van cascading style sheets (CSS) om inhoud onzichtbaar te maken voor de ontvanger, maar wel aanwezig in de HTML-code. Door manipulatie van CSS-eigenschappen zoals font-grootte, zichtbaarheid en containerafmetingen kunnen aanvallers verborgen inhoud toevoegen die traditionele detectiesystemen misleiden. De aanvallen komen steeds vaker voor in phishingcampagnes, scams en geavanceerde bedreigingen die gericht zijn op waardevolle organisaties. De methode is bijzonder effectief tegen zowel handtekeninggebaseerde oplossingen als geavanceerde machine learning-modellen die tekstanalyses gebruiken. Onderzoekers hebben geconstateerd dat deze techniek veel vaker voorkomt in kwaadaardige e-mails dan in legitieme communicatie. Dit vereist dat organisaties verbeterde detectie- en filtratiesystemen implementeren die rekening houden met CSS-gebaseerde inhoudsverberging.

Shuyal Stealer richt zich op 19 browsers om inloggegevens te stelen

Shuyal Stealer is een geavanceerd malwareprogramma dat in snel tempo als een veelzijdige tool voor het stelen van inloggegevens is opgekomen. Het werd voor het eerst gedetecteerd in augustus 2025 en heeft sindsdien honderden systemen in

verschillende sectoren gecompromitteerd, waaronder financiën, gezondheidszorg en productie. De malware maakt gebruik van social engineering, bijvoorbeeld via phishing-e-mails of kwaadaardige advertenties. Het wordt gedistribueerd als een software-update of hulpprogramma, waarbij een DLL-loader wordt gebruikt om de malafide code te injecteren in de browserprocessen. Shuyal Stealer kan inloggegevens, cookies en opgeslagen wachtwoorden stelen uit 19 verschillende browsers, waaronder Chrome, Firefox en Edge. Gegevens worden vervolgens versleuteld en via HTTPS verzonden naar een dynamisch gegenereerd subdomein. Het gebruik van een DLL-side-loading techniek helpt de malware detectie te omzeilen door geen verdachte bestanden op de schijf te plaatsen.

Velociraptor gebruikt bij ransomware-aanvallen

Cisco heeft bevestigd dat de open-source DFIR-tool Velociraptor wordt misbruikt bij ransomware-aanvallen. Deze tool, ontwikkeld door Rapid7, wordt normaal ingezet voor digital forensics en incident response, maar wordt nu door aanvallers gebruikt om toegang te verkrijgen tot systemen. Velociraptor stelt aanvallers in staat om stealthy toegang te behouden en de LockBit- en Babuk-ransomware te verspreiden. De aanvallers installeren een verouderde versie van Velociraptor, die kwetsbaarheden bevat (CVE-2025-6264). Deze kwetsbaarheid kan door aanvallers worden gebruikt om hun rechten op het systeem te verhogen, willekeurige commando's uit te voeren en volledige controle over het endpoint te verkrijgen. Onderzoekers adviseren organisaties om het ongeautoriseerd gebruik van Velociraptor nauwlettend te monitoren en te onderzoeken.

Oracle EBS-lek gebruikt voor grootschalige afpersingscampagne

Sinds augustus wordt een kritieke kwetsbaarheid in Oracle E-Business Suite (EBS) misbruikt door criminelen voor een grootschalige afpersingscampagne. Het lek, CVE-2025-61882, stelt aanvallers in staat om op afstand code uit te voeren op getroffen servers zonder enige authenticatie. Criminelen hebben gegevens van EBS-servers gestolen en dreigen deze openbaar te maken tenzij er losgeld wordt betaald. Google en The Shadowserver Foundation bevestigen dat honderden EBS-servers wereldwijd nog steeds kwetsbaar zijn, ondanks een patch die Oracle op 4 oktober uitbracht. De FBI heeft organisaties opgeroepen het lek onmiddellijk te patchen. Momenteel zijn veel getroffen servers te vinden in de VS, China, India en Duitsland.

Nieuwe ransomwaregroep geïdentificeerd: Brotherhood

Een nieuwe ransomwaregroep genaamd "Brotherhood" is geïdentificeerd op het Dark Web. Deze groep heeft een nieuwe locatie opgezet voor hun activiteiten, bereikbaar via een .onion-domein. De groep lijkt zich te richten op het verspreiden van ransomware-aanvallen met als doel het verkrijgen van losgeld van slachtoffers. Er zijn geen specifieke gegevens vrijgegeven over de slachtoffers of de gebruikte methoden, maar de groep heeft een aantal berichten gepost met informatie over hun aanvallen. Dit komt kort na een periode van verhoogde ransomware-activiteit op het Dark Web, waar verschillende groepen met soortgelijke tactieken opereren.

Onderzoek naar gerichte “payroll pirate” aanvallen op Amerikaanse universiteiten

Microsoft Threat Intelligence heeft een financieel gemotiveerde dreigingsactor, Storm-2657, geïdentificeerd die zich richt op universiteiten in de VS. Deze aanvallen, bekend als “payroll pirate”, gebruiken social engineering om toegang te krijgen tot werknemersprofielen en salarissen om te leiden naar gecontroleerde bankrekeningen van de aanvaller. Het doelwit zijn voornamelijk werknemers van instellingen in het hoger onderwijs die via platforms voor personeelsbeheer zoals Workday worden aangevallen. De aanvallen maken gebruik van phishing-e-mails die ontworpen zijn om MFA-codes te stelen. Zodra de aanvaller toegang heeft tot de accounts, worden inboxregels aangemaakt om waarschuwingen van systemen zoals Workday te verwijderen. Microsoft raadt het gebruik van phishing-resistente MFA aan om deze aanvallen te voorkomen. Affected klanten kunnen door Microsoft ondersteund worden in hun mitigatie-inspanningen.

Nieuwe ClayRat-spyware richt zich op Android-gebruikers via valse WhatsApp- en TikTok-apps

Een nieuwe vorm van Android-spyware, ClayRat, richt zich momenteel op gebruikers in Rusland. De malware wordt verspreid via Telegram-kanalen en valse phishing-websites die populaire apps zoals WhatsApp, Google Foto’s, TikTok en YouTube imiteren. Zodra geïnstalleerd, kan de spyware SMS-berichten, oproepgeschiedenissen en apparaat-informatie stelen, foto's maken met de frontcamera en zelfs berichten versturen of oproepen plaatsen vanaf het

slachtofferapparaat. Daarnaast verspreidt de malware zichzelf door schadelijke links naar alle contacten in de telefoonlijst van het slachtoffer te sturen. ClayRat heeft binnen 90 dagen meer dan 600 monsters en 50 droppers gedetecteerd, waarbij elke versie nieuwe technieken gebruikt om detectie te omzeilen. De malware maakt gebruik van valse updates om gebruikers te misleiden, en de infectie wordt via beveiligingslekken verder verspreid naar andere apparaten.

hackercollectief 'trinity of chaos' lekt gegevens van 39 bedrijven, waaronder google en cisco

Het hackercollectief Trinity of Chaos heeft een dataleksite opgezet op het TOR-netwerk, waar het gevoelige informatie van 39 grote bedrijven is gepubliceerd. De groep, die wordt verondersteld leden van de bekende cybercriminelen zoals Lapsus$, Scattered Spider en ShinyHunters te omvatten, heeft ransomware-tactieken gecombineerd met datadiefstal om financiële druk uit te oefenen op hun slachtoffers. Onder de gecompromitteerde bedrijven bevinden zich grote namen zoals Google, Cisco, Toyota en FedEx. De groep heeft de slachtoffers een ultimatum gesteld, met als dreiging de publicatie van nog meer data als ze niet voldoen aan de eisen. De meeste gelekte gegevens bevatten persoonlijke informatie, maar bevatten geen wachtwoorden. Trinity of Chaos richt zich op bedrijven in sectoren zoals technologie, financiën en telecommunicatie wereldwijd, en gebruikt geavanceerde social engineering technieken om toegang te verkrijgen.

AI-chatbot gebruikt als backdoor voor toegang tot gevoelige gegevens en infrastructuur

In de afgelopen weken is er een geavanceerde malwarecampagne ontdekt waarbij conversatie-AI-chatbots werden misbruikt als verborgen toegangspunten tot bedrijfssystemen. De aanvallers richtten zich op organisaties die chatapplicaties op basis van grote taalmodellen gebruikten. Door zwakheden in de natuurlijke taalverwerking en indirecte gegevensinvoer te exploiteren, konden de aanvallers onterecht toegang krijgen tot systemen. In eerste gevallen werden financiële instellingen aangevallen, waar een publieke chatbot per ongeluk schadelijke inhoud van externe beoordelingssites inslikte, wat leidde tot een keten van privilege-escalaties. De aanvallers gebruikten foutmeldingen van de chatbot om informatie te verkrijgen over de onderliggende systemen en een verborgen injectie van code uit te

voeren, waarmee ze toegang kregen tot interne API's en gevoelige klantgegevens. Detectie van deze tactieken vereist constante monitoring en integriteitscontrole van scripts en geplande taken binnen de IT-infrastructuur.

Chaos ontstaat door snellere, slimmere en gevaarlijkere ransomware

Een nieuwe ransomwarevariant heeft in de afgelopen weken wereldwijd voor veel problemen gezorgd. Deze ransomware, die eind september 2025 voor het eerst werd opgemerkt, versleutelt binnen enkele seconden na uitvoering gegevens, waardoor er weinig tijd is voor tegenmaatregelen. Sectoren zoals de gezondheidszorg, financiën en productie melden grootschalige uitval van systemen door aanvallen via onbeveiligde RDP-sessies en phishing-e-mails. Het malwareprogramma maakt gebruik van een aangepaste loader die zich via kwetsbare RDP-sessies verspreidt en zich verstopt in DLL-modules, wat snelle verspreiding door netwerken mogelijk maakt. Forensisch onderzoek toont aan dat de ransomware snel en efficiënt werkt, met versleuteling in minder dan 30 seconden voor 10 GB data op moderne systemen. De aanvallers vragen losgeld in Monero, met bedragen die op maat zijn gemaakt voor het slachtoffer. De malware is uiterst moeilijk te detecteren door traditionele antivirussoftware, vanwege zijn geoptimaliseerde code en polymorfisme.

Werknemer die wegens hacken op staande voet werd ontslagen verliest kort geding

Een werknemer van een fietswinkelketen verloor een kort geding waarin hij eisde doorbetaling van zijn salaris na ontslag op staande voet wegens hackpogingen. In juni werden er pogingen gedaan om via een usb-stick malware op laptops van de keten te installeren. De medewerker was de enige aanwezig op het moment van de detectie, wat leidde tot zijn ontslag. De fietswinkel beweerde dat hij verantwoordelijk was voor de hackpogingen, inclusief het meenemen van een laptop. De kantonrechter oordeelde dat het ontslag goed onderbouwd was en dat de medewerker onvoldoende verklaring gaf voor de gebeurtenissen die plaatsvonden na zijn vertrek. De vordering om het ontslag te vernietigen werd afgewezen, en de werknemer moest de proceskosten van 949 euro betalen.

Ziekenhuis ontslaat medewerkers wegens ongeoorloofd inzien patiëntendossiers

Het Albert Schweitzer Ziekenhuis heeft twee medewerkers ontslagen voor het ongeoorloofd inzien van elfhonderd patiëntendossiers. De medewerkers hadden geen behandelrelatie met de patiënten en verklaarden dat ze uit nieuwsgierigheid de dossiers hadden bekeken. Het ziekenhuis ontdekte de incidenten tijdens controles op het elektronisch patiëntendossier. Bestuursvoorzitter Nicole Stolk benadrukte dat het vertrouwen van patiënten in de veiligheid van hun gegevens essentieel is, en dat dergelijk gedrag niet geaccepteerd wordt. Het ziekenhuis voert sinds jaren controles uit, maar heeft besloten deze verder te intensiveren. Ook werd de Autoriteit Persoonsgegevens en de Inspectie Gezondheidszorg en Jeugd ingelicht, en zijn alle getroffen patiënten geïnformeerd.

Aanhouding van verdachte door onderschepte gegevens criminele organisaties

De politie heeft een 39-jarige man uit Hoogvliet aangehouden, verdacht van betrokkenheid bij de handel in harddrugs en witwassen. Het onderzoek, gestart in maart 2025, richtte zich op de handel van grote hoeveelheden cocaïne en geld witwassen. Door eerder onderschepte berichten via de versleutelde berichtendienst Sky ECC kwam de politie de verdachte op het spoor. Tijdens het onderzoek werden meerdere locaties doorzocht, waaronder woningen in Hoogvliet en Schiedam, en een bedrijfspand in Hoogvliet. Daarbij werden kilo's harddrugs, geld en gegevensdragers in beslag genomen. De verdachte werd op 7 oktober aangehouden en wordt binnenkort voorgeleid aan de Rechter-Commissaris. Het onderzoek maakt gebruik van gegevens die zijn verkregen uit Sky ECC, een platform dat in 2021 werd gekraakt en sindsdien bijgedragen heeft aan diverse arrestaties.

Discord vermoedt dat het id-bewijzen van 70.000 gebruikers zijn gelekt

Discord heeft recentelijk een datalek gemeld waarbij vermoedelijk de identiteitsbewijzen van 70.000 gebruikers zijn gestolen. Het lek werd veroorzaakt door een aanval op een externe klantenserviceplatform, vermoedelijk Zendesk. De aanvallers zouden 1,5 terabyte aan leeftijdsverificatiegerelateerde foto's hebben buitgemaakt, waaronder paspoort- en rijbewijsafbeeldingen, gebruikersnamen, e-mailadressen, en andere persoonlijke gegevens. Discord heeft bevestigd dat het om een klein aantal gebruikers gaat, maar de exacte aantallen zijn nog niet volledig duidelijk. De gehackte gegevens bevatten ook vier laatste cijfers van creditcardnummers, IP-adressen, en berichten naar supportmedewerkers. Discord

onderzoekt de zaak verder en is bezig om de getroffen gebruikers te informeren. Het platform heeft echter aangegeven niet in te zullen gaan op de losgeld eisen van de aanvallers.

Denemarken schrapt stemming over chatcontrole in de EU

Denemarken heeft besloten de stemming over het voorstel voor chatcontrole uit te stellen, nadat het niet genoeg voorstemmers had kunnen krijgen. Het voorstel had tot doel chatberichten van Europese burgers te controleren, maar stuitte op verzet van een grote groep EU-lidstaten. Ondanks eerdere pogingen door landen zoals België, Polen en Hongarije om vergelijkbare maatregelen door te voeren, bleek ook deze poging geen meerderheid te vinden. De stemming was gepland voor 14 oktober, maar wordt uitgesteld omdat de “blokkerende minderheid” te groot is. Dit voorstel, gesteund door de Europese Commissie, wordt gezien als een bedreiging voor de privacy van burgers. Tegenstanders roepen op tot het intrekken van het plan. Er wordt verwacht dat een toekomstige EU-voorzitter opnieuw een poging zal doen om het voorstel in te voeren.

Waarschuwing voor Europese plannen die privacy bedreigen

Het Woerdense cybersecuritybedrijf Vallem waarschuwt voor de implicaties van een aankomend wetsvoorstel van de Europese Commissie tegen cybercriminaliteit. Dit voorstel zou de privacy van Europese burgers ernstig kunnen aantasten. Volgens Vallem zou de wet ervoor zorgen dat de overheid steeds meer toegang krijgt tot privédata van burgers, zoals reisinformatie en persoonlijke communicatie via apps. Het bedrijf stelt dat deze wet zou leiden tot een 'digitale gevangenis', waarbij de persoonlijke vrijheid van gebruikers in de digitale ruimte sterk beperkt wordt. Als reactie heeft Vallem een petitie gestart om de grondrechten van de Nederlandse burger te beschermen. De bezorgdheid over de wet groeit, aangezien de Europese Commissie deze maand een besluit zou nemen over het wetsvoorstel.

Scattered LAPSUS$ Hunters claim breaches of global firms including Dell and Verizon

De cybercrime-groep Scattered LAPSUS$ Hunters, een fusie van Scattered Spider, LAPSUS$ en ShinyHunters, heeft recentelijk meerdere grote internationale bedrijven

gehackt, waaronder Dell, Verizon, Telstra en Kuwait Airways. De groep heeft voorbeelden van gestolen gegevens gepubliceerd, waaronder persoonlijke informatie zoals namen, adressen, telefoonnummers, geboortedata, e-mailadressen, werkposities en paspoortnummers. Deze gegevens zouden het risico op identiteitsdiefstal, gerichte oplichting en sociale manipulatie vergroten. Scattered LAPSUS$ Hunters richt zich voornamelijk op grote multinationals vanwege de omvangrijke databronnen en complexe netwerken die vatbaar zijn voor aanvallen. De groep heeft naar verluidt bijna een miljard records gestolen en dreigt data van meer dan 700 bedrijven openbaar te maken, tenzij betaling wordt ontvangen. De recente aanvallen komen nadat de groep eerder een nep “pensioen” aankondigde, maar ondertussen alweer actief is met nieuwe afpersingscampagnes.

Microsoft werkt aan herstel na Azure-uitval die toegang tot Microsoft 365 blokkeerde

Microsoft werkt aan het herstel van een storing die de toegang tot verschillende Microsoft 365-diensten heeft geblokkeerd. De storing, veroorzaakt door problemen met het Azure Front Door content delivery network, begon om 07:40 UTC en had invloed op klanten in Europa, Afrika en het Midden-Oosten. Gebruikers ondervonden vertragingen en time-outs bij het verbinden met de Azure- en Entra-portalen. Microsoft heeft sindsdien Kubernetes-instanties opnieuw opgestart om de capaciteit te herstellen. Ongeveer 98% van de getroffen diensten zijn hersteld, maar enkele gebruikers ervaren nog steeds intermitterende problemen. Het incident wordt actief gevolgd op de Service Health Dashboard. Er zijn geen exacte cijfers bekend over het aantal getroffen klanten. Microsoft heeft beloofd de resterende 4% van de getroffen klanten zo snel mogelijk te herstellen.

Ongewenste abonnementen na valse (win)acties

Er zijn steeds meer meldingen van valse (win)acties die leiden tot ongewenste abonnementen. Dit betreft bijvoorbeeld acties waarbij consumenten iets kunnen winnen of ontvangen, en waarvoor ze gegevens moeten invullen en een klein bedrag betalen, vaak via een creditcard. Dit resulteert onbewust in het afsluiten van dure abonnementen met hoge maandlasten. Deze valse acties verschijnen via advertenties op sociale media, vervalste e-mails of verkoop langs de deur, waarbij QR-codes op deelnameformulieren zijn gemanipuleerd. De Fraudehelpdesk waarschuwt om geen linkjes in e-mails of advertenties te volgen, geen QR-codes te

scannen en geen (creditcard)gegevens in te vullen. Het advies is om loten of producten die aan de deur worden verkocht altijd via de officiële website van de aanbieder aan te schaffen.

Qilin ransomware-groep lanceert 70 aanvallen in 30 dagen

De Qilin ransomware-groep, ook wel bekend als Agenda, is sinds 2022 actief als een ransomware-as-a-service (RaaS) platform. In de afgelopen maand (augustus-september 2025) heeft de groep 70 aanvallen uitgevoerd op verschillende sectoren wereldwijd, waaronder overheden, gezondheidszorg, scholen en financiële instellingen. De aanvallen raakten onder andere bedrijven in de Verenigde Staten, Europa, Zuid-Korea en Afrika. Qilin gebruikt ransomware die zowel Windows-, Linux- als ESXi-systemen kan infecteren. Het blijkt dat de groep zich niet richt op één sector, maar een breed scala aan doelwitten aanvalt. Het gebruik van gestolen inloggegevens, phishing en kwetsbaarheden in openbare systemen stelt Qilin in staat om een wereldwijd netwerk van aanvallen uit te voeren. Organisaties worden geadviseerd om maatregelen zoals multi-factor authenticatie en regelmatige patchupdates in te voeren om zich te beschermen tegen deze dreiging.