Cybercrimeinfo - cyberdreigingsanalyse (Openbare versie)

17-10-2025:

Chinese groep 'Jewelbug' infiltreert Russisch IT-netwerk

De Chinese hacker groep 'Jewelbug' heeft zich maandenlang stilletjes toegang verschaft tot een Russisch IT-dienstverleningsbedrijf, van januari tot mei 2025. De groep maakte gebruik van Microsoft-hulpmiddelen en heeft gegevens geëxfiltreerd via Yandex Cloud. De aanvallen werden onderzocht door het bedrijf Symantec, dat Jewelbug koppelt aan andere bekende Chinese bedreigingsactoren. De inbraak heeft de toegang verschaft tot belangrijke code repositories en softwarebuildsystemen, wat de mogelijkheid creëert voor toekomstige supply chain-aanvallen. Bij de aanval werd een aangepaste versie van Microsoft Console Debugger gebruikt, wat het mogelijk maakte om beveiligingsmaatregelen te omzeilen en schadelijke code te draaien. Het gebruik van cloudservices en legitieme tools toont de voorkeur van Jewelbug voor een subtiele en langdurige aanwezigheid op slachtoffernetwerken, wat de detectie bemoeilijkt. Dit incident benadrukt de voortdurende dreiging van Chinese cyberoperaties, zelfs tegenover landen met sterkere diplomatieke banden met China.

Rusland, China gebruiken AI voor cyberaanvallen op de VS

Rusland, China, Iran en Noord-Korea maken steeds meer gebruik van kunstmatige intelligentie (AI) om online misleiding te verspreiden en cyberaanvallen uit te voeren op de Verenigde Staten. Microsoft ontdekte in juli 2025 meer dan 200 gevallen van buitenlandse tegenstanders die AI gebruikten voor het creëren van valse content, een verdubbeling ten opzichte van het jaar ervoor. Deze landen en andere kwaadwillende actoren gebruiken AI om cyberaanvallen te automatiseren, desinformatie te verspreiden en gevoelige systemen te penetreren. De aanvallen richten zich vaak op overheden, bedrijven en kritieke infrastructuur, zoals ziekenhuizen en vervoersnetwerken. AI maakt het mogelijk om phishing-e-mails te verbeteren en digitale kloons van regeringsfunctionarissen te creëren. Microsoft waarschuwt dat bedrijven en organisaties hun cyberbeveiliging moeten versterken, aangezien AI de dreigingen in cyberspace versnelt.

Noord-Koreaanse hackers gebruiken EtherHiding om malware op blockchain te verbergen

Noord-Koreaanse hackers hebben de EtherHiding-techniek geïntroduceerd, waarmee ze malware kunnen verbergen in slimme contracten op publieke blockchains zoals Ethereum en Binance Smart Chain. Deze methode, die sinds februari 2025 door de DPRK wordt gebruikt, maakt het mogelijk om kwaadaardige scripts te hosten en te distribueren zonder dat er zichtbare transacties zijn, waardoor de aanvallen moeilijker te detecteren zijn. De hackers richten zich voornamelijk op softwareontwikkelaars door middel van valse sollicitatiegesprekken, waarbij de slachtoffers schadelijke code uitvoeren die vervolgens malware downloadt. De eerste fase van de infectie gebruikt een downloader, gevolgd door een tweede fase waarbij gegevens zoals inloggegevens en crypto-wallet-informatie worden gestolen. EtherHiding biedt anonimiteit, lage kosten en de mogelijkheid om payloads te updaten, waardoor de aanvallen zeer flexibel en moeilijk te traceren zijn.

MI5 Chief: VK Confronteert Groeiende Dreiging van Rusland, Iran en China

De Britse binnenlandse inlichtingendienst MI5 staat onder druk door de toenemende dreigingen van Rusland, Iran en China. MI5-directeur Ken McCallum meldde een stijging van 35% in het aantal personen die worden onderzocht voor staatsdreigingen. Volgens McCallum is de organisatie in 2025 geconfronteerd met een grotere en gevarieerdere dreiging van zowel terroristen als statelijke actoren dan ooit tevoren. Hij benadrukte dat landen zoals Rusland, Iran en China steeds vaker “de agressieve methoden” gebruiken die MI5 eerder alleen in terreurzaken tegenkwam. McCallum verwees ook naar de voortdurende online campagnes van Rusland die gericht zijn op het testen van de kwetsbaarheden binnen de Britse samenleving. Daarnaast waarschuwde hij voor de toenemende cyberspionage vanuit China en de pogingen van Iran om critici het zwijgen op te leggen. MI5 blijft waakzaam om deze dreigingen tegen te gaan.

VS meldt actief misbruik van kritiek lek in Adobe Experience Manager Forms

Adobe Experience Manager Forms heeft te maken met een kritieke kwetsbaarheid (CVE-2025-54253), die het mogelijk maakt om remote code execution uit te voeren. Deze kwetsbaarheid is beoordeeld met een score van 10.0 op een schaal van 1 tot 10, wat aangeeft dat het een zeer ernstige dreiging vormt. Hoewel Adobe op 5 augustus 2025 een beveiligingsupdate uitbracht, werd kort daarna proof-of-concept exploitcode openbaar gedeeld. Het Cybersecurity and Infrastructure Security Agency

(CISA) van de VS heeft nu bevestigd dat er daadwerkelijk misbruik van deze kwetsbaarheid plaatsvindt. Adobe Experience Manager wordt gebruikt door organisaties om digitale formulieren te beheren en te integreren met andere Adobe-oplossingen. De kwetsbaarheid wordt toegeschreven aan een misconfiguratie die de uitvoering van willekeurige code mogelijk maakt. Amerikaanse overheidsinstanties moeten de update voor 5 november implementeren.

Amerikaanse overheid beveelt installatie F5 BIG-IP-updates vanwege dreiging

De Amerikaanse overheid heeft een noodbevel afgegeven waarin federale instanties worden verplicht om beveiligingsupdates voor F5 BIG-IP-producten binnen een week te installeren. Dit volgt op een inbraak bij F5, waarbij aanvallers broncode en informatie over niet-bekende kwetsbaarheden buitmaakten. F5 heeft daarop verschillende updates uitgebracht om de kwetsbaarheden te verhelpen. Het BIG-IP-platform wordt gebruikt voor load balancing en application delivery. Het Cybersecurity and Infrastructure Security Agency (CISA) waarschuwt dat de gestolen informatie kan leiden tot aanvallen op overheidsnetwerken. Als de kwetsbaarheden misbruikt worden, kunnen aanvallers toegang krijgen tot gevoelige gegevens en informatiesystemen volledig compromitteren. Het CISA beschouwt de situatie als een "onacceptabel risico" en verplicht federale instanties om snel actie te ondernemen, met deadlines voor de installatie van updates op 22 en 31 oktober 2025.

PoC-exploit voor NTLM-reflectie SMB-kwetsbaarheid gepubliceerd

Op 15 oktober 2025 werd een PoC-exploit gedeeld voor de NTLM-reflectie SMB-kwetsbaarheid (CVE-2025-33073) op GitHub. Deze kwetsbaarheid kan misbruikt worden in Microsoft-omgevingen, wat leidt tot potentieel gevaarlijke aanvallen via SMB-protocollen. De publicatie bevat zowel een grafische als commandoregelinterface (GUI en CLI), evenals op maat gemaakte commando's en SOCKS-functionaliteit voor het uitvoeren van de exploit. De kwetsbaarheid, die bekend staat om zijn vermogen om netwerkbeveiligingen te omzeilen, heeft ernstige implicaties voor systemen die deze configuraties gebruiken. De beveiligingscommunity wordt aangespoord om proactief te patchen en relaybeschermingen in te stellen om schade te voorkomen. Deze publicatie heeft veel aandacht getrokken, aangezien het een breed gebruik van de SMB-protocollen binnen bedrijfsomgevingen raakt.

PoC code voor IngressNightmare kwetsbaarheden vrijgegeven

De kwetsbaarheden IngressNightmare, aangeduid als CVE-2025-1097, CVE-2025-1098, CVE-2025-24514 en CVE-2025-1974, zijn recent ontdekt en er is nu PoC-code (Proof of Concept) beschikbaar om deze kwetsbaarheden te exploiteren. Deze kwetsbaarheden zijn gerelateerd aan de beveiliging van systemen die gebruik maken van de IngressNightmare configuratie, welke kunnen leiden tot ernstige beveiligingsrisico's. De code is gedeeld op GitHub en kan door aanvallers gebruikt worden om toegang te krijgen tot gevoelige systemen. Organisaties wordt aangeraden deze kwetsbaarheden onmiddellijk te onderzoeken en te patchen om schade te voorkomen. Aangezien de PoC-code beschikbaar is gesteld, is het belangrijk om snel actie te ondernemen om de systemen te beschermen tegen mogelijke aanvallen.

Hackers gebruiken Cisco SNMP-kwetsbaarheid om Linux rootkits te verspreiden via 'Zero Disco'-aanvallen

Hackers hebben een nieuwe aanvalscampagne gelanceerd die gebruik maakt van een kwetsbaarheid in Cisco IOS Software en IOS XE Software, aangeduid als CVE-2025-20352. Deze kwetsbaarheid maakt het mogelijk voor een aanvaller om op afstand willekeurige code uit te voeren door speciaal gemaakte SNMP-pakketten naar kwetsbare apparaten te sturen. De aanvallen, bekend als 'Zero Disco', richten zich vooral op oudere Cisco-apparaten zoals de 9400, 9300 en 3750G series. De hackers implementeren Linux rootkits die persistente toegang bieden door universele wachtwoorden in te stellen en hooks te installeren in de Cisco IOSd-processen. Deze rootkits maken het mogelijk voor aanvallers om onder de radar te opereren, vooral op systemen zonder endpoint-detectie en reactie-oplossingen. Cisco heeft de kwetsbaarheid inmiddels gepatcht, maar de aanvallen werden uitgevoerd als zero-day exploits.

Kritieke kwetsbaarheden in Windows BitLocker onthuld

Microsoft heeft twee kritieke kwetsbaarheden in de Windows BitLocker-versleuteling openbaar gemaakt. Deze kwetsbaarheden stellen aanvallers in staat om beveiligingsmaatregelen te omzeilen en versleutelde gegevens te benaderen als ze

fysiek toegang hebben tot het apparaat. De kwetsbaarheden, aangeduid als CVE-2025-55338 en CVE-2025-55333, werden op 14 oktober 2025 gepatcht in de maandelijkse Patch Tuesday-updates. Beide kwetsbaarheden hebben een "Belangrijke" ernstclassificatie en een CVSS-score van 6,1, wat wijst op het risico van datalekken bij diefstal of manipulatie van apparaten. De problemen hebben te maken met het niet kunnen patchen van ROM-code en onvolledige vergelijkingen van gegevens, wat het mogelijk maakt ongeautoriseerde toegang zonder wachtwoorden of herstelcodes. Microsoft adviseert dringend de update toe te passen, vooral voor mobiele werkers en risicovolle omgevingen.

Fortinet brengt patches uit voor meerdere kwetsbaarheden in producten

Fortinet heeft op 16 oktober 2025 kritieke patches uitgebracht voor verschillende van haar producten, waaronder FortiOS, FortiPAM, en FortiSwitch Manager. De patches verhelpen meerdere kwetsbaarheden, waaronder een privilege escalation (CVE-2025-58325) en een authenticatieomzeiling (CVE-2025-49201), die beide kunnen worden misbruikt door aanvallers om toegang te krijgen tot systemen of gevoelige gegevens. De kwetsbaarheden zijn beoordeeld met een hoge CVSS-score, met CVE-2025-49201 die een score van 9.8 heeft. Hoewel er geen aanwijzingen zijn dat deze kwetsbaarheden al zijn misbruikt, adviseert de CCB dringend om de patches onmiddellijk toe te passen. Naast de kritieke kwetsbaarheden zijn er ook medium- en laag-risico kwetsbaarheden aangepakt. Organisaties wordt aangeraden om de updates met prioriteit toe te passen en verdachte activiteiten nauwlettend te monitoren.

Ontdekking van kwetsbaarheid in Rust-gebaseerde Windows-kernelcomponent

In januari 2025 ontdekte Check Point Research een kwetsbaarheid in de nieuwe Rust-gebaseerde kernelcomponent van de Windows Graphics Device Interface (GDI). Deze kwetsbaarheid werd snel aan Microsoft gemeld, die de bug verholpen heeft in OS Build 26100.4202, onderdeel van de update KB5058499. De kwetsbaarheid werd ontdekt via fuzzing van metafiles, waarbij herhaaldelijke systeemcrashes, genaamd "Denial of Fuzzing", optraden. De oorzaak bleek een bug in de Windows-kernel die werd getriggerd door een onveilige verwerking van GDI-metadata. De exploitatie van deze bug zou kunnen leiden tot systeemcrashes of zelfs gegevensverlies. Microsoft classifyerde de kwetsbaarheid als een "moderatere"

storing, maar implementeerde een beveiligingsupdate die het probleem oploste. Deze ontdekking benadrukt de noodzaak van rigoureuze beveiligingstests, zelfs bij gebruik van geheugenveilige programmeertalen zoals Rust.

Nepbeveiligingsmeldingen van LastPass en Bitwarden leiden tot pc-overnames

Er is een lopende phishingcampagne die zich richt op gebruikers van LastPass en Bitwarden. De aanvallers versturen valse e-mails waarin wordt beweerd dat de bedrijven gehackt zijn en dat gebruikers een veiliger desktopversie van hun wachtwoordmanager moeten downloaden. De e-mails bevatten links naar een schadelijke binary die het Syncro-platform installeert, een tool voor remote monitoring en management. Dit platform wordt gebruikt om ScreenConnect, software voor externe ondersteuning, te deployen, waardoor de aanvallers volledige toegang krijgen tot de pc van het slachtoffer. Zowel LastPass als Bitwarden hebben bevestigd dat er geen beveiligingsincidenten hebben plaatsgevonden en waarschuwen voor de valse meldingen. De nepberichten proberen urgentie te creëren en gebruikers over te halen een onveilige versie van de software te installeren. Beide bedrijven adviseren gebruikers altijd via officiële kanalen in te loggen om de veiligheid te verifiëren.

Non-webprotocollen worden nieuwe aanvalsvectoren

Aanvallers richten zich steeds vaker op niet-webprotocollen zoals DNS, RDP en SMB om netwerken te infiltreren. Traditionele beveiligingssystemen kunnen deze aanvallen moeilijk detecteren, aangezien de aanvallers gebruikmaken van tunneling en andere verborgen communicatietechnieken via deze protocollen. Recent onderzoek van Zscaler onthult dat DNS misbruik de grootste dreiging vormt, goed voor 83,8% van de niet-webbedreigingen. Daarnaast nemen brute force-aanvallen tegen RDP en SMB sterk toe, vooral gericht op verouderde systemen. De detailhandel is de meest getroffen sector, gevolgd door kritieke infrastructuren zoals energie en productie, waar SSH-aanvallen rampzalige gevolgen kunnen hebben. Anonimiseringshulpmiddelen zoals Tor verergeren de dreiging door aanvallers te helpen hun activiteiten te verbergen. Het rapport benadrukt dat de toename van gerichte aanvallen, specifiek aangepast aan sectoren, cybercriminelen in staat stelt om hun winstgevendheid te vergroten. Het gebruik van een Zero Trust-aanpak kan helpen om deze nieuwe aanvalsvectoren effectief te neutraliseren.

PhantomVAI Loader valt wereldwijd organisaties aan om AsyncRAT, XWorm, FormBook en DCRat te verspreiden

Een geavanceerde, multi-stage malwarecampagne maakt gebruik van de PhantomVAI Loader om verschillende informatie-diefstalmalsware zoals AsyncRAT, XWorm, FormBook en DCRat te verspreiden. Deze aanvallen beginnen met zorgvuldig samengestelde phishing-e-mails, die gericht zijn op bedrijven in sectoren zoals productie, gezondheidszorg, technologie en overheidsinstellingen. De malware, voorheen bekend als de Katz Stealer Loader, maakt gebruik van geavanceerde technieken om e-mailbeveiligingsfilters te omzeilen, inclusief homograafaanvallen, waarbij visueel vergelijkbare tekens worden gebruikt. De aanval is bijzonder gevaarlijk doordat de malwarescripts sterk geobfuseerd zijn, en Base64-gecodeerde PowerShell-commando's bevatten die automatisch worden uitgevoerd zodra de verdachte bijlagen worden geopend. Zodra de aanval succesvol is, wordt de malware gedownload van een aanvallersserver en ingebed in legitieme systeembestanden, waardoor de malware verborgen blijft terwijl het gevoelige informatie steelt.

Microsoft: meeste cyberaanvallen via exploits en gestolen wachtwoorden

Microsoft heeft in zijn jaarlijkse Digital Defense Report gemeld dat de meeste cyberaanvallen in 2024 plaatsvonden door het gebruik van exploits voor kwetsbaarheden en gestolen wachtwoorden. Ongeveer 37 procent van de incidenten was gericht op datadiefstal, gevolgd door afpersing (33 procent) en ransomware (19 procent). In 11 procent van de gevallen was exploitatie van kwetsbare software de initiële toegangsmethode, terwijl hetzelfde percentage werd veroorzaakt door gestolen inloggegevens. Social engineering speelde een rol in 10 procent van de incidenten. Microsoft merkt op dat toegangsmakelaars, die systemen binnendringen en de toegang doorverkopen aan andere criminelen, vaak een sleutelrol spelen in ransomware-aanvallen. De meerderheid van deze aanvallen maakt gebruik van gestolen inloggegevens, voornamelijk afkomstig van datalekken of infostealer-malware. Microsoft benadrukt het belang van phishingbestendige multifactorauthenticatie als maatregel tegen dergelijke aanvallen.

LinkPro Linux rootkit gebruikt eBPF om zich te verbergen en wordt geactiveerd via magische TCP-pakketten

Een onderzoek naar een gecompromitteerde infrastructuur op Amazon Web Services (AWS) heeft de ontdekking van een nieuw Linux-rootkit, genaamd LinkPro, onthuld. Het rootkit maakt gebruik van eBPF-modules (extended Berkeley Packet Filter) om zichzelf te verbergen en wordt geactiveerd wanneer een specifiek TCP-pakket wordt ontvangen. Het kwaadwillige pakket heeft een "magische" waarde in het venster van het TCP-pakket (54321), wat de communicatie met het command-and-control (C2) systeem mogelijk maakt. LinkPro kan in twee modi werken: passief, waarbij het wacht op een specifiek TCP-pakket, en actief, waarbij het zelf verbinding maakt met het C2-systeem. Het rootkit maakt gebruik van verschillende technieken om zijn aanwezigheid te verbergen, waaronder het manipuleren van systeemaanroepen en het aanpassen van netwerkverkeer. De aanval begon via een kwetsbare Jenkins-server en gebruikte een kwaadaardige Docker-afbeelding.

Hackers misbruiken blockchain smart contracts voor verspreiding van malware via geïnfecteerde WordPress-sites

Een financieel gemotiveerde dreigingsactor, UNC5142, maakt gebruik van blockchain smart contracts om informatie steler-malwaresoftware zoals Atomic, Lumma en Vidar te verspreiden via geïnfecteerde WordPress-websites. Het proces, genaamd "EtherHiding", verbergt kwaadaardige code op publieke blockchains, zoals de BNB Smart Chain. UNC5142 richt zich op zowel Windows- als macOS-systemen en maakt gebruik van een meerfasige JavaScript-downloader, genaamd CLEARSHORT, die malware in twee stadia verspreidt via geïnfecteerde websites. Dit proces omvat het ophalen van een landingpagina van een smart contract op de blockchain en het misleiden van slachtoffers om schadelijke commando's uit te voeren. De techniek biedt bescherming tegen detectie en verwijdering door zijn interactie met de blockchain. Ondanks een pauze in activiteiten in juli 2025, blijven de campagnes geavanceerd en weerbaar tegen beëindiging.

Qilin ransomware gebruikt Ghost bulletproof hosting voor wereldwijde aanvallen

De Qilin ransomware-groep heeft zich gepositioneerd als een van de meest gevaarlijke cyberdreigingen, die gebruikmaakt van geavanceerde bulletproof hosting-infrastructuur om wereldwijde organisaties aan te vallen. Oorspronkelijk begonnen in 2022 onder de naam Agenda, richt de groep zich op een breed scala aan sectoren, waaronder gezondheidszorg, overheden, kritieke infrastructuren en

vermogensbeheer. Onlangs was de groep verantwoordelijk voor de aanval op Asahi Group, Japan's grootste drankproducent, die productie onderbrak in de meeste van haar fabrieken. Qilin maakt gebruik van zowel de programmeertalen Golang als Rust voor zijn ransomware-aanvallen, wat zorgt voor veelzijdigheid en cross-platform aanvalsmogelijkheden. De groep past de tactiek van dubbele extortie toe, waarbij gegevens worden versleuteld en tegelijkertijd worden gestolen om druk uit te oefenen op de slachtoffers. De ransomware-operatie werkt samen met ondergrondse bulletproof hostingproviders, die een veilige haven bieden voor deze activiteiten.

Nieuwe phishingaanval gebruikt Basic Auth-URL's om gebruikers te misleiden en inloggegevens te stelen

Begin oktober 2025 werd een oude phishingtechniek opnieuw gebruikt, waarbij Basic Authentication-URL's werden ingezet om gebruikers te misleiden en hun inloggegevens te stelen. De aanvallers maakten links in de vorm van https://gebruikersnaam:wachtwoord@domein.com, waarbij het domein van een vertrouwde instelling in het gebruikersnaamveld werd verborgen. Wanneer gebruikers op deze links klikten, werden hun browsers geauthenticeerd op het kwaadwillende domein, waarna hun inloggegevens werden verzameld. Deze techniek is vooral effectief in mobiele apps en e-mailclients, die lange URL's inkorten. De eerste aanvallen richtten zich op klanten van GMO Aozora Bank in Japan, maar ook andere grote merken zoals Amazon, Google en Netflix werden geïmiteerd. De aanvallers gebruikten een CAPTCHA-pagina om de slachtoffers verder te misleiden en de legitimiteit van de pagina te verhogen. De gebruikte Basic Auth-URL's ontsnapten aan reguliere URL-filters, wat deze aanvalslijn moeilijk te detecteren maakt.

Operatie silk lure maakt gebruik van windows task scheduler om valleyrat te verspreiden

Operation Silk Lure is een gerichte campagne die de Windows Taakplanner misbruikt om een nieuwe variant van de ValleyRAT-malware te verspreiden. De aanval, die zich richt op de HR-afdelingen van Chinese fintech- en handelsbedrijven, begint met spear-phishing-e-mails die schadelijke LNK-bestanden bevatten die zich voordoen als sollicitatiebrieven. Wanneer deze bestanden worden geopend, wordt een verborgen PowerShell-commando uitgevoerd, dat een loader (keytool.exe) en een

DLL (jli.dll) downloadt. Na de initiële infectie registreert een VBScript een dagelijks geplande taak die de loader uitvoert en persistente toegang creëert. De malware maakt vervolgens verbinding met een command-and-control-server en verzamelt gegevens, terwijl beveiligingsmaatregelen van antivirussoftware worden omzeild. Het gebruik van DLL-side-loading en het maskeren van de activiteiten maakt deze operatie bijzonder moeilijk te detecteren.

Nieuwe phishing-aanval misbruikt Microsoft-urls om gebruikers te verleiden tot inloggen

Cybercriminelen hebben een nieuwe phishing-aanvalstechniek ontwikkeld waarbij ze Microsoft-urls gebruiken om slachtoffers te misleiden. De aanval vindt plaats via een link die lijkt te verwijzen naar forms.office.com, maar uiteindelijk leidt naar een kwaadaardige website. Daar wordt het slachtoffer gevraagd in te loggen met hun M365-account, waarna de criminelen toegang kunnen krijgen tot de gegevens. Wat deze techniek gevaarlijk maakt, is dat de URL eindigt op windows.net, wat het lijkt alsof de link legitiem is, hoewel het dit niet is. Het is belangrijk voor gebruikers om altijd te controleren of de inlogpagina de juiste URL bevat (login.microsoftonline.com) en alert te zijn op verdachte links.

Politie waarschuwt voor fraude via telefoonnummers die op politienummer lijken

De politie heeft een waarschuwing uitgegeven voor fraudeurs die gebruikmaken van telefoonnummers die lijken op het officiële politienummer 0900-8844. Deze fraudepogingen worden uitgevoerd met nummers als 900-8844 of +31900-8844. Wanneer mensen dit nummer in hun display zien, denken ze wellicht dat ze door de politie worden gebeld, maar dit is niet het geval. De criminelen proberen slachtoffers op te lichten door zich voor te doen als politieagenten. Slachtoffers krijgen te maken met fraudeurs die hen in sommige gevallen vragen om een kleine betaling voor een pakketje, terwijl in andere gevallen de oplichters zich als nepagenten voordoen en persoonlijke informatie proberen te verkrijgen, zoals pincodes. De politie raadt aan de verbinding direct te verbreken en geen informatie te verstrekken.

Afperser PowerSchool krijgt 4 jaar cel en moet 14 miljoen dollar betalen

Een 20-jarige Amerikaan is in de VS veroordeeld tot vier jaar gevangenisstraf en moet 14 miljoen dollar schadevergoeding betalen na het hacken van systemen van PowerSchool, een grote aanbieder van onderwijssoftware. De verdachte stal persoonlijke gegevens van miljoenen studenten en leraren, wat resulteerde in een afpersing van 2,85 miljoen dollar. PowerSchool betaalde losgeld, maar de gegevens bleven uiteindelijk in het bezit van de aanvaller. De verdachte had via gestolen inloggegevens toegang gekregen tot de systemen van PowerSchool. De zaak kwam aan het licht toen de aanvaller ook een Amerikaanse telecomprovider afperste en klantgegevens buitmaakte. De verdachte bekende in juni schuld en werd uiteindelijk veroordeeld. Het incident benadrukt de kwetsbaarheid van cloudsystemen voor onderwijsinstellingen en de opkomst van afpersing via gestolen gegevens.

GoGetSMS mogelijk in beslag genomen door autoriteiten

GoGetSMS, een populaire online dienst voor het verkrijgen van tijdelijke telefoonnummers, lijkt recentelijk in beslag genomen te zijn. Gebruikers die de website bezoeken, zien een pagina die zich draait en hen achter tralies toont, hoewel de reden voor deze actie onduidelijk blijft. Er is momenteel geen officiële verklaring of nieuwsbericht beschikbaar over de situatie, wat de speculatie voedt dat dit mogelijk een gestage inbeslagname is. Terwijl enkele gebruikers de banner als nep beschouwen, blijft het onbekend of de inbeslagname een tijdelijke actie of een permanente sluiting van de site betreft. Het incident roept vragen op over de betrokkenheid van autoriteiten en de implicaties voor gebruikers van dergelijke diensten, maar verdere details zijn nog niet openbaar.

Politie arresteert twee vrouwen in onderzoek naar datingfraude met schade van meer dan €550.000

Op 15 oktober 2025 heeft de politie twee vrouwen uit Utrecht aangehouden in een onderzoek naar datingfraude. Het onderzoek begon in juni 2025 na tientallen aangiftes van slachtoffers, waarvan 26 meldingen tussen juni 2022 en september 2025 werden geregistreerd. De verdachten, vrouwen van 26 en 41 jaar, zouden via een datingplatform slachtoffers hebben opgelicht door een valse relatie te creëren en hen vervolgens geld of goederen af te persen. De schade bedraagt ruim €550.000. Tijdens fysieke ontmoetingen werden slachtoffers gedwongen betalingen te doen. Na de aanhoudingen werden drie locaties in Utrecht doorzocht, waarbij onder andere

geld, sieraden en een auto in beslag werden genomen. Meer aanhoudingen worden niet uitgesloten. Slachtoffers van soortgelijke fraude kunnen zich melden bij de politie.

IT-specialisten en kinderen werken aan echte politiezaken in vijfde editie Hackathon

Op 10 oktober vond de vijfde editie van de Hackathon plaats, waarin ruim 80 digitale topspecialisten samenwerkten aan echte politiezaken. Deelnemers onderzochten diverse onderwerpen, zoals cold cases, vermissingszaken en gedigitaliseerde criminaliteit. Een nieuw onderdeel van de Hackathon was het kinderteam, bestaande uit jonge talenten, dat zich richtte op phishingwebsites. De kinderen werkten samen met ervaren specialisten om criminelen te stoppen die wachtwoorden en gegevens stelen. De teams onderzochten ook zaken als nepagenten, boilerroomfraude en bankhelpdeskfraude. Deelnemers uit Zweden, Duitsland en het Verenigd Koninkrijk namen deel, wat het belang van internationale samenwerking benadrukte. Aan het einde van de dag werden verschillende aanknopingspunten gepresenteerd, waaronder het opsporen van criminelen achter nepwebsites en het vinden van nieuwe sporen in onopgeloste zaken, zoals een Amber Alert.

Europol breekt illegaal online goknetwerk met bijna 1 miljard euro aan omzet op

Twee verdachten van het runnen van verschillende illegale online casinowebsites zijn aangeklaagd en vastgezet in Frankrijk. De autoriteiten werden gealarmeerd nadat slachtoffers zich meldden over het niet kunnen opnemen van hun winsten. De samenwerking tussen verschillende landen, waaronder Cyprus, was essentieel voor het ontrafelen van de frauduleuze activiteiten. Het onderzoek onthulde dat het goknetwerk in de afgelopen vijf jaar bijna 1 miljard euro aan omzet had gegenereerd. Ondanks waarschuwingen van de Franse autoriteiten en de moeilijkheden voor slachtoffers om hun winsten op te nemen, werd er verdacht van witwassen. Er werden tussen 2022 en 2025 meer dan 100 miljoen euro aan geldtransfers vastgesteld. Dankzij de samenwerking tussen de landen werden er acties ondernomen, zoals huiszoekingen en bevriezing van activa. De verdachten werden op 9 oktober in Frankrijk aangeklaagd voor illegaal gokken, witwassen en deelname aan een criminele organisatie.

Prosper lekt persoonlijke gegevens van 17,6 miljoen gebruikers

Kredietplatform Prosper heeft persoonlijke gegevens van 17,6 miljoen gebruikers gelekt, waaronder inkomensgegevens, kopieën van identiteitsbewijzen, social-securitynummers, namen, adressen, e-mailadressen, geboortedatums, kredietstatus, IP-adressen, arbeidssituaties en browserinformatie. Prosper biedt via zijn platform leningen aan tussen 2.000 en 50.000 dollar. De inbraak vond vorige maand plaats, waarbij een aanvaller toegang kreeg tot de systemen en verschillende gegevens buitmaakte. Prosper heeft geen details gegeven over hoe de inbraak plaatsvond. De gestolen e-mailadressen zijn inmiddels opgenomen in de datalekzoekmachine "Have I Been Pwned". Van deze e-mailadressen was 84 procent al eerder via andere datalekken bekend. Gebruikers kunnen via de zoekmachine controleren of hun gegevens zijn aangetast.

Amerikaanse senator vraagt om meer informatie van Cisco over kwetsbaarheden in netwerkapparatuur

De Amerikaanse senator Bill Cassidy heeft Cisco gevraagd om meer informatie over twee kwetsbaarheden die actief worden aangevallen. Deze kwetsbaarheden bevinden zich in de Cisco Secure Firewall Adaptive Security Appliance (ASA) en Cisco Secure Firewall Threat Defense (FTD) software. De kwetsbaarheden kunnen door aanvallers worden misbruikt om volledige controle over de apparaten te verkrijgen. De Amerikaanse overheid gaf op 25 september een "emergency directive" uit, waarin overheidsinstanties werden opgedragen deze kwetsbaarheden binnen 24 uur te patchen. Cassidy heeft Cisco-topman Chuck Robbins gevraagd duidelijk te maken hoe het bedrijf proactief informatie deelt over de aanvallen en of klanten met verouderde apparaten geadviseerd worden deze offline te halen. De senator heeft Cisco tot 27 oktober de tijd gegeven om de vragen te beantwoorden.

Dota 2 YouTube-account tijdelijk gehackt voor promotie Solana meme coin

Het officiële YouTube-kanaal van Dota 2 werd op woensdag kort gehackt, waarbij een livestream werd gepromoot die de Solana-gebaseerde token "dota2coin" aanbood. De livestream, getiteld "Dota 2 Launch Official Meme Coin | Hurry Up," bevatte een link naar een zogenaamde PumpFun-token. De video was snel verwijderd, maar niet voordat het kwaadwillende initiatief werd gedocumenteerd door gebruikers op Reddit. Er zijn geen aanwijzingen dat gebruikersdata werd gestolen.

De hack volgt een bekend patroon van eerdere YouTube-kanaalovernames waarbij frauduleuze crypto-aanbiedingen worden gepromoot. Dit incident komt ook te midden van meldingen van technische problemen bij YouTube, waarbij sommige gebruikers geen toegang hadden tot video's. De waarde van de meme coin daalde snel, met een marktkapitalisatie van ongeveer $5,500, wat een daling van 21% vertegenwoordigt sinds de lancering van de token.

Verkoop van crypto-drainer tool op Dark Web opgemerkt

Op 15 oktober 2025 werd via een bericht van de Dark Web Informer een vermeende verkoop van een crypto-drainer tool op het Dark Web gemeld. De tool is specifiek gericht op Tron- en EVM-gebaseerde cryptocurrencies, waarmee kwaadwillenden de crypto-wallets van slachtoffers kunnen leeghalen. Deze tool, die wordt aangeboden voor verkoop, maakt gebruik van slimme contracten om toegang te krijgen tot de wallet-adressen van slachtoffers en hen van hun cryptovaluta te beroven. De verkoop van dergelijke tools is een zorgwekkende ontwikkeling, aangezien het de potentiële dreiging van opkomende cybercriminaliteit vergroot, gericht op cryptomunten. Dit incident benadrukt wederom de voortdurende groei van de crypto-gerelateerde cybercriminaliteit op het Dark Web, en het belang van waakzaamheid en beveiliging voor gebruikers van digitale valuta.

TorZon Darknet Market toegevoegd aan Dread Superlist

TorZon, een Darknet-markt, is toegevoegd aan de Dread Superlist, een lijst van goedgekeurde en betrouwbare marktplaatsen. Deze marktplaatsen worden gezien als verifieerbaar en opereren in goede trouw, hoewel het advies blijft om voorzichtig te zijn bij het gebruik ervan. De vermelding op de Dread Superlist komt nadat de markt is beoordeeld en blijkt te voldoen aan de vereisten van betrouwbaarheid binnen de Dark Web-gemeenschap. Gebruikers worden nog steeds aangeraden om voorzichtig te handelen, aangezien het gebruik van deze marktplaatsen risico’s met zich meebrengt, ondanks hun vermeende betrouwbaarheid. De officiële aankondiging van deze status is te vinden op de aangegeven Darknet-link.

Nintendo meldt dat er geen data is buitgemaakt bij recente hack

Nintendo heeft bevestigd dat er geen bewijs is dat bij de recente hack gebruikersdata of bedrijfsinformatie is gestolen. De hack vond plaats op externe servers die de websites van het bedrijf hosten, waarbij sommige servers "gedefaced" werden. Nintendo reageerde hiermee op de hackersgroep Crimson Collective, die beweerde verantwoordelijk te zijn voor de aanval. De groep had een screenshot gedeeld van mappen op de servers, maar zonder verdere details over wat er mogelijk is buitgemaakt. Nintendo heeft nog niet gereageerd op de gepubliceerde screenshot, maar benadrukt dat er geen schadelijke gevolgen zijn van de aanval. De situatie benadrukt echter de noodzaak voor bedrijven om hun netwerken goed te beveiligen tegen dergelijke inbraken, zelfs als er geen gegevens zijn gestolen.

Nieuwe tech support scam misbruikt Microsoft-logo om browser te blokkeren en gegevens te stelen

Een nieuwe tech support scam, ontdekt door het Cofense Phishing Defense Centre, maakt misbruik van het vertrouwen in het Microsoft-logo om slachtoffers te misleiden. Deze scam begint met een e-mail die een nepteruggave of vergoeding aanbiedt en de ontvanger naar een valse CAPTCHA-pagina leidt. Na deze stap wordt de browser van het slachtoffer gemanipuleerd om een ‘browser lock’ te tonen, wat de indruk wekt van een ransomware-aanval. De scam maakt gebruik van angst om slachtoffers te dwingen het nep-Microsoft-ondersteuningsnummer te bellen. Wanneer het slachtoffer belt, wordt het verbonden met een frauduleuze technicus die probeert inloggegevens te stelen of toegang tot de computer te verkrijgen via remote desktop-software. Het doel is gegevensdiefstal en systeeminfiltratie, waarbij het merk Microsoft als vertrouwenswapen wordt ingezet. Slachtoffers moeten alert blijven en nooit onverwacht een nummer bellen dat in een pop-up verschijnt.

Microsoft trekt tweehonderd certificaten in gebruikt door ransomwaregroep

Microsoft heeft deze maand meer dan tweehonderd certificaten ingetrokken die door de ransomwaregroep "Vanilla Tempest" werden gebruikt voor het digitaal signeren van malafide bestanden. De bestanden, die zich voordeden als installatiebestanden van Microsoft Teams, bevatten een backdoor waarmee de Rhysida-ransomware werd uitgerold. De aanvallers maakten gebruik van de code signing diensten van Trusted Signing, SSL.com, DigiCert en GlobalSign. De groep, die ook bekendstaat als Vice Society, gebruikte zoekmachineoptimalisatie (SEO) poisoning om malafide

domeinen zoals "teams-download" en "teams-install" hoger in zoekresultaten te krijgen, zodat slachtoffers de bestanden zouden downloaden. Microsoft waarschuwt voor het gebruik van deze technieken door cybercriminelen om systemen aan te vallen.

Dark Web: Verkoop van stuurprogramma met toegang tot fysieke geheugen

Op 16 oktober 2025 werd op het Dark Web melding gemaakt van de vermeende verkoop van een stuurprogramma dat toegang biedt tot het fysieke geheugen van computersystemen. Deze ontdekking werd gedeeld via een bericht van de account 'Dark Web Informer' op X (voorheen Twitter). Het stuurprogramma zou kunnen worden ingezet voor cyberaanvallen waarbij de toegang tot fysieke geheugenlocaties op apparaten een belangrijke rol speelt. Dit soort informatie kan een ernstig risico vormen voor de veiligheid van systemen, aangezien het de mogelijkheid biedt voor diepgaande toegang tot gevoelige gegevens en het omzeilen van beveiligingsmaatregelen. De verkoop van dergelijke stuurprogramma's geeft aan dat de dreigingen op het Dark Web zich blijven ontwikkelen, wat een toenemende bezorgdheid wekt binnen de cybersecuritygemeenschap over de bescherming van kritieke infrastructuren en systemen.