Cybercrimeinfo - cyberdreigingsanalyse (Openbare versie)

13-11-2025:

Ferocious Kitten APT zet MarkiRAT in voor het vastleggen van toetsaanslagen en klembordgegevens

De Iraans gelinkte APT-groep Ferocious Kitten richt zich sinds 2015 op Perzisch-sprekende doelwitten, voornamelijk dissidenten en activisten. De groep gebruikt politiek geladen documenten om slachtoffers te misleiden en schadelijke bestanden uit te voeren. Het belangrijkste instrument is de MarkiRAT-malware, die uitgebreide gegevensverzamelcapaciteiten biedt, waaronder het vastleggen van toetsaanslagen, klembordgegevens, screenshots en wachtwoordinzamelingen. De aanvallen worden uitgevoerd via spearphishing-campagnes waarbij gemanipuleerde Microsoft Office-documenten worden verzonden met ingebedde macros. Zodra een slachtoffer een document opent, wordt de malware uitgevoerd, waarmee een persistentie wordt gevestigd. MarkiRAT maakt gebruik van verschillende techniek om detectie te omzeilen, waaronder het manipuleren van bestandsnamen om schadelijke bestanden als onschuldige media te verbergen. De malware verzamelt niet alleen gevoelige informatie maar richt zich ook specifiek op wachtwoorden en versleutelde bestanden, wat de dreiging verder vergroot.

Chef Defensie: België lijkt focus van verhoogde hybride dreiging

Volgens Chef Defensie Frederik Vansina lijkt België momenteel het doelwit te zijn van een verhoogde hybride dreiging. Hij wees op recente incidenten met drones boven luchthavens en militaire domeinen, cyberdreigingen, en de verhoogde aanwezigheid van schepen voor de kust. Daarnaast wordt er een groeiende "assertieve retoriek" op sociale media waargenomen, mogelijk aangestoken door buitenlandse actoren. Vansina benadrukte dat dergelijke hybride dreigingen in heel Europa zichtbaar zijn, met aanwijzingen dat Rusland betrokken zou zijn, onder andere bij sabotages van onderzeese kabels en cyberaanvallen. De generaal riep op tot versnelling van defensie-investeringen en technologieën om deze dreigingen tegen te gaan, zoals het tegengaan van drones. De internationale situatie, zoals de oorlog in Oekraïne en de technologische vooruitgang, maakt de dreiging in Europa steeds complexer.

Hackers misbruiken Citrix- en Cisco ISE-kwetsbaarheden in zero-day aanvallen

Geavanceerde dreigingsactoren hebben de kritieke kwetsbaarheden "Citrix Bleed 2" (CVE-2025-5777) in NetScaler ADC en Gateway, en CVE-2025-20337 in Cisco Identity Service Engine (ISE) uitgebuit als zero-days voor het implementeren van op maat gemaakte malware. De aanval werd gedetecteerd door Amazon's threat intelligence team, dat ontdekte dat de kwetsbaarheden al werden misbruikt vóór de publieke bekendmaking en de beschikbaarheid van patches. De Citrix-kwetsbaarheid, die een geheugenlekkage veroorzaakte, werd in juni gepatcht, terwijl de kwetsbaarheid in Cisco ISE, die pre-authenticatie toegang verleende, in juli werd aangekondigd. De aanvallers gebruikten deze kwetsbaarheden om een op maat gemaakte webshell te installeren, waarmee ze ongeautoriseerde toegang verkregen tot systemen. Deze aanvallen wijzen op een goed georganiseerde en goed uitgeruste dreigingsactor. Het wordt aanbevolen om de beschikbare beveiligingsupdates onmiddellijk toe te passen.

Danabot malware duikt op met versie 669 na operatie Endgame

Danabot, een bekende banking trojan, is teruggekeerd met versie 669 na een tijdelijke onderbreking door de handhavingsactie Operation Endgame in mei 2025. Deze geavanceerde malware richt zich opnieuw op financiële instellingen, cryptocurrency-gebruikers en individuele slachtoffers via geavanceerde multi-stage aanvallen. De trojan maakt gebruik van spear-phishing en kwaadaardige documenten om systemen te infecteren, waarna het zijn payload aflevert. Zodra de malware zich heeft gevestigd, kan het meerdere modules inzetten voor gegevensdiefstal, laterale verplaatsing binnen netwerken en verdere payload-levering, specifiek voor Windows-omgevingen. Danabot versie 669 heeft ook zijn infrastructuur geüpdatet, waarbij het nu zowel IP-gebaseerde command-and-control (C2)-servers als .onion-adressen gebruikt voor communicatie, wat de detectie bemoeilijkt. Deze strategische verbeteringen maken de malware een nog grotere dreiging in het huidige cyberlandschap.

Grote phishingaanval via Meta Business Suite richt zich op MKB-gebruikers wereldwijd

Een grootschalige phishingaanval is ontdekt die zich richt op gebruikers van Meta Business Suite, met als doel inloggegevens te stelen van duizenden kleine en middelgrote bedrijven wereldwijd. De aanval, die werd geïdentificeerd door Check

Point-onderzoekers, verspreidde ongeveer 40.000 phishing-e-mails naar meer dan 5.000 klanten, voornamelijk uit de automobiel-, onderwijs-, vastgoed-, horeca- en financiële sectoren in de VS, Europa, Canada en Australië. De phishingcampagne maakt gebruik van legitieme Meta-infrastructuur, wat het moeilijker maakt om de aanval te detecteren. Aanvallers maakten misbruik van de uitnodigingsfunctie van Meta Business, waardoor de berichten authentiek lijken en traditionele e-mailbeveiligingsfilters omzeilen. De e-mails bevatten schadelijke links die gebruikers naar phishing-websites leiden, waar inloggegevens en andere gevoelige informatie wordt verzameld. Organisaties wordt geadviseerd om multi-factorauthenticatie in te schakelen om ongeautoriseerde toegang te voorkomen.

Phishingcampagne via @facebookmail.com richt zich op Facebook Business-gebruikers

Een nieuwe phishingcampagne maakt misbruik van het officiële @facebookmail.com-domein om Facebook Business-gebruikers wereldwijd te misleiden. De aanvallers verstuurden e-mails die lijken op officiële uitnodigingen van Meta, bedoeld om de ontvangers naar frauduleuze inlogpagina's te lokken. Deze e-mails, met onderwerpen zoals 'Accountverificatie vereist' en 'Uitnodiging voor Meta Agency Partner', bevatten links naar websites die ontworpen zijn om inloggegevens van gebruikers te stelen. De campagne werd opgemerkt door Check Point en heeft wereldwijd duizenden kleine en middelgrote bedrijven getroffen, waaronder bedrijven in de VS, Europa, Canada en Australië. Het grootste slachtoffer ontving meer dan 4.000 phishingberichten. Bedrijven die gebruik maken van Meta Business Suite wordt geadviseerd om multi-factor authenticatie in te schakelen en uitnodigingen altijd te verifiëren via de officiële Meta-ondersteuningspagina’s.

Nieuwe KomeX Android RAT geadverteerd op hackerforums met abonnementsopties

Een nieuwe Android Remote Access Trojan (RAT), genaamd KomeX, is opgedoken op hackerforums en zorgt voor bezorgdheid binnen de cybersecuritygemeenschap. Het is gebouwd op de BTMOB RAT-code en biedt geavanceerde spionage- en apparaatcontrolefuncties. KomeX wordt gepromoot door een dreigingsactor onder de alias “Gendirector” en is ontworpen om Android-apparaten in massa te infecteren. De malware wordt verspreid via schadelijke Android-apps en phishingcampagnes. Na installatie vraagt KomeX onmiddellijk om uitgebreide systeemrechten, wat zijn bereik

vergroot en zijn effectiviteit versterkt. De RAT biedt onder andere functies voor live schermstreaming, audio- en videocaptatie via camera en microfoon, sms-interceptie, geolocatie-tracking, en volledige besturingssysteemtoegang. KomeX wordt verkocht met verschillende abonnementsopties, waaronder toegang voor een korte periode, levenslange updates en volledige broncode voor criminele netwerken die aangepaste aanpassingen willen maken.

Authentication Coercion-aanval manipuleert Windows-machines om inloggegevens te onthullen

Een nieuwe vorm van cyberaanval, bekend als 'authentication coercion', richt zich op Windows-systemen binnen organisaties. Deze aanval maakt gebruik van de ingebouwde communicatieprotocollen in Windows om machines te misleiden en gevoelige inloggegevens automatisch naar een door de aanvaller gecontroleerde server te sturen. De techniek is bijzonder effectief doordat het gebruik maakt van legitieme Windows-functies, zoals Remote Procedure Call (RPC), wat het moeilijk maakt voor traditionele beveiligingssystemen om de aanval te detecteren. De aanvallers zetten kwaadaardige luisteraars op die zich voordoen als vertrouwde netwerkbronnen. Wanneer een geïnfecteerde machine probeert verbinding te maken met deze server, worden de inloggegevens via RPC-berichten doorgestuurd. Aangezien de aanval geen speciale rechten vereist, kunnen aanvallers met minimale technische kennis profiteren van deze kwetsbaarheid. Organisaties kunnen zichzelf beschermen door verdachte RPC-patronen en ongebruikte protocollen te monitoren en beveiligingsmaatregelen zoals SMB-handtekeningen in te stellen.

Hackers gebruiken AppleScript voor macOS-malware via Zoom/Teams-updates

Hackers hebben een nieuwe methode ontwikkeld om malware te verspreiden via AppleScript-bestanden (.scpt), die nu worden gebruikt om vervalste Zoom- en Teams-installaties te verspreiden. Deze bestanden worden gepresenteerd als legitieme software-updates, maar bevatten schadelijke code. Wanneer gebruikers de bestanden openen, wordt een sociaal-engineeringprompt weergegeven, die hen aanmoedigt de scriptbestanden uit te voeren, zelfs als ze door Apple’s Gatekeeper-beveiliging zijn gemarkeerd. De aanvallers maken gebruik van de scripteditor van macOS, een legitieme applicatie die door gebruikers vaak wordt vertrouwd. Deze aanvalsmethode is moeilijk te detecteren, aangezien veel van de AppleScript-

bestanden momenteel geen meldingen op virus-scanners zoals VirusTotal geven. Security-onderzoekers hebben dit als een zorgwekkende trend gemeld, vooral omdat deze techniek nu ook door cybercriminelen wordt gebruikt die eerder geavanceerde aanvallen uitvoerden.

Nieuwe phishingaanval maakt misbruik van populaire merken om inloggegevens te stelen

Een geavanceerde phishingcampagne richt zich op organisaties in Centraal- en Oost-Europa door legitieme wereldmerken te imiteren om gebruikers te misleiden en hun inloggegevens te verkrijgen. De aanval maakt gebruik van zelfbevatte HTML-bestanden die als e-mailbijlagen worden verzonden, waardoor externe servers of verdachte URL's, die meestal door traditionele beveiligingssystemen worden gedetecteerd, overbodig zijn. Wanneer de bijlagen worden geopend, tonen ze overtuigende nep-inlogpagina's voor merken zoals Microsoft 365, Adobe, WeTransfer, FedEx en DHL, waarmee een naadloze gebruikerservaring wordt gecreëerd. Deze aanpak maakt gebruik van JavaScript binnen de HTML-bestanden om inloggegevens te verzamelen en direct naar Telegram-bots van de aanvallers te sturen. De campagne richt zich vooral op sectoren zoals landbouw, de auto-industrie, de bouw en het onderwijs in landen als Tsjechië, Slowakije, Hongarije en Duitsland. Organisaties wordt aangeraden om controles voor HTML-bijlagen in te voeren om dergelijke aanvallen te blokkeren.

APT-C-08 hackers gebruiken WinRAR-kwetsbaarheid om overheden aan te vallen

De APT-C-08 hacker-groep, ook bekend als Manlinghua of BITTER, heeft een verfijnde aanvalscampagne gelanceerd gericht op overheidsorganisaties in Zuid-Azië. De groep maakt gebruik van een kritieke directory traversal-kwetsbaarheid in WinRAR (CVE-2025-6218), die het mogelijk maakt om systeemgrenzen te doorbreken en kwaadaardige code uit te voeren op gecompromitteerde systemen. De groep heeft een lange geschiedenis in het stelen van gevoelige informatie van overheidsinstanties en andere gerelateerde organisaties. De aanval maakt gebruik van een speciaal gemaakte RAR-archief met misleidende bestandsnamen, zoals "Provision of Information for Sectoral for AJK[.]rar". Wanneer het archief wordt uitgepakt, wordt een kwaadaardig macrobestand gedeponeerd op het systeem, dat via Microsoft Word automatisch wordt geladen. Experts raden aan alle WinRAR-

installaties onmiddellijk te patchen en toepassing van macro-uitvoering te blokkeren voor verhoogde bescherming.

Malicious SteamCleaner-aanval richt zich op Windows-machines met backdoor malware

Een nieuwe aanval richt zich op Windows-gebruikers via een gemanipuleerde versie van SteamCleaner, een legitiem hulpprogramma voor het opruimen van ongewenste bestanden van het Steam-platform. De malware maakt gebruik van Node.js-scripts om toegang te verkrijgen tot het systeem en onderhoudt communicatie met command-and-control-servers. Deze aanval maakt gebruik van een ongewijzigde versie van het SteamCleaner-programma, dat sinds 2018 geen updates meer heeft ontvangen, maar nu wordt verspreid via frauduleuze websites. Het kwaadaardige installatiebestand is ondertekend met een geldig digitaal certificaat, waardoor het aanvankelijk niet wordt gedetecteerd door beveiligingssoftware. Nadat het programma is uitgevoerd, installeert de malware zich op het systeem en zorgt ervoor dat er verbinding wordt gemaakt met meerdere C2-servers voor verdere commando-uitvoering. De aanvallers maken gebruik van geavanceerde technieken om detectie te voorkomen, zoals het uitvoeren van milieutests en het obfusceren van commando's.

Toename van macOS infostealers: nieuwe dreiging voor Apple-gebruikers

In 2025 is er een significante stijging in het gebruik van infostealers gericht op macOS-apparaten, wat een verhoogde dreiging vormt voor zowel individuele gebruikers als bedrijven. Deze malware is ontworpen om vertrouwelijke gegevens zoals inloggegevens, cryptowallets en persoonlijke informatie te stelen. Door de groeiende populariteit van macOS, vooral in zakelijke omgevingen, zijn deze apparaten nu een aantrekkelijk doelwit voor cybercriminelen. KELA’s onderzoek toont aan dat de macOS-gebruikers vaak hogere inkomens hebben, meer vertrouwen in de beveiliging van hun apparaten en waardevolle accounts beheren, wat hen kwetsbaarder maakt voor social engineering-aanvallen. Bedrijven die macOS in hun netwerk gebruiken lopen het risico dat één gecompromitteerd apparaat toegang biedt tot gevoelige gegevens, waaronder cloud- en SaaS-inloggegevens. De markt voor macOS infostealers heeft zich ontwikkeld tot een gestructureerd ecosysteem waarin dergelijke malware tegen hoge prijzen wordt verhandeld.

Massale phishingcampagne misleidt gebruikers met 4.300 malafide domeinen

Een grootschalige phishingcampagne richt zich wereldwijd op reizigers door meer dan 4.300 valse domeinen te gebruiken om betaalkaartgegevens te stelen. De aanvallers doen zich voor als bekende reismerken en sturen nepbevestigingsmails voor hotelboekingen, waarmee ze slachtoffers naar valse boekingspagina's lokken. De nepwebsites zijn zorgvuldig ontworpen om legitiem te lijken, met bekende logo's en professionele layouts. De slachtoffers worden aangemoedigd om snel te handelen en hun gegevens in te voeren, onder de indruk van valse urgentie. De aanval maakt gebruik van een complex redirectiesysteem, waarbij de slachtoffers via meerdere websites naar de phishingpagina worden geleid. Zodra de slachtoffers hun betaalgegevens invoeren, worden deze gestolen. De aanval wordt toegeschreven aan een Russisch-talige dreigingsactor. De campagne, die begon in februari 2025, is in omvang gegroeid met dagelijks nieuwe domeinen.

Drie oplichters aangehouden na poging bankhelpdeskfraude

Dinsdagavond zijn drie personen gearresteerd na een poging tot bankhelpdeskfraude. De mannen deden zich voor als medewerkers van een bank en benaderden een slachtoffer telefonisch. Ze beweerden dat er geld van zijn rekening was gepind, terwijl de eigenaar van de bankpas dit ontkende. Later werd ontdekt dat er een bedrag van de creditcard was afgehaald, maar de betalingen werden gelukkig tegengehouden. Het slachtoffer twijfelde aan het verhaal en waarschuwde de politie, die snel actie ondernam. De zogenaamde koerier, die onderweg was om de bankpassen op te halen, werd voor de deur aangehouden. Twee andere verdachten werden in de nabije omgeving opgepakt. De verdachten zijn een 18-jarige man uit Amsterdam, een 18-jarige man uit Diemen en een 17-jarige vrouw uit Amsterdam. Deze aanhoudingen onderstrepen het belang van waakzaamheid bij telefoontjes van vermeende banken.

65-plussers gebruiken tweestapsverificatie minder vaak dan gemiddeld

Uit recent onderzoek blijkt dat Nederlanders vooral gebruik maken van tweestapsverificatie (2FA) bij overheidsdiensten (77%), medische diensten (64%) en financiële diensten (59%). Er is echter een opvallend verschil tussen

leeftijdsgroepen: 65-plussers gebruiken 2FA minder vaak dan jongere generaties. Zo past 66% van hen 2FA toe bij overheidsdiensten, tegenover 77% van de algemene bevolking, en slechts 49% bij financiële diensten, tegenover 59% gemiddeld. De meerderheid van de ouderen vindt 2FA te veel gedoe of heeft er simpelweg nooit aan gedacht. Dit komt doordat zij vaak minder bewust zijn van de risico's van ongeautoriseerde toegang tot hun online accounts. Eind november start de overheid een campagne gericht op het verhogen van het bewustzijn over de voordelen van 2FA voor deze groep.

AP deelt aanbevelingen voor een sterke verwerkersovereenkomst bij een cyberaanval

De Autoriteit Persoonsgegevens (AP) heeft recent aanbevelingen gedeeld voor het opstellen van een sterke verwerkersovereenkomst, gericht op het verbeteren van de samenwerking tussen organisaties en hun dienstverleners bij cyberaanvallen. Een verwerkersovereenkomst bevat afspraken over het delen van persoonsgegevens en de verantwoordelijkheden bij datalekken. De AP benadrukt dat dienstverleners vaak het doelwit zijn van cyberaanvallen, mede door hun rol in meerdere organisaties, wat de schade vergroot. Bij onderzoek naar vijf grote cyberaanvallen werd geconcludeerd dat het ontbreken van adequate verwerkersovereenkomsten vaak leidde tot een beperkte grip op het incident. De AP raadt aan om duidelijke afspraken te maken over taken en communicatie bij datalekken, grip te houden op de leveranciersketen, en verwerkersovereenkomsten regelmatig bij te werken om de risico's van cyberincidenten te verkleinen.

VK scherpt cybersecuritywetgeving aan voor vitale sectoren

Het Britse parlement heeft een wetsvoorstel ingediend dat vitale sectoren zoals ziekenhuizen, energieleveranciers, waterbedrijven en transportnetwerken beter moet beschermen tegen cyberaanvallen. De nieuwe Cyber Security and Resilience Bill verplicht organisaties in deze sectoren, evenals bedrijven die IT-diensten leveren, om strengere beveiligingsmaatregelen te nemen. Organisaties moeten ernstige cyberincidenten binnen 24 uur melden en binnen 72 uur een volledig rapport indienen bij hun toezichthouder en het National Cyber Security Centre (NCSC). Ook worden datacenters en digitale dienstverleners verplicht om getroffen klanten onmiddellijk te waarschuwen na een incident. De wet voorziet in nieuwe

bevoegdheden voor toezichthouders om kritieke leveranciers aan te wijzen, en bedrijven die openbare diensten leveren moeten voldoende bescherming bieden om de continuïteit van hun systemen te waarborgen. Overtredingen kunnen leiden tot omzetgerelateerde boetes.

Active Directory blijft topdoelwit voor cyberaanvallen

Active Directory (AD) speelt een cruciale rol in de beveiliging van bedrijfssystemen en wordt door cybercriminelen vaak aangevallen. AD beheert de toegang tot netwerken door middel van gebruikersauthenticatie en autorisatie. Zodra aanvallers AD compromitteren, krijgen zij toegang tot het hele netwerk, waarmee ze accounts kunnen aanmaken, machtigingen kunnen wijzigen en beveiligingsinstellingen kunnen uitschakelen. Dit vergroot de risico's op een ernstige aanval, zoals bleek bij de cyberaanval op Change Healthcare, waarbij de aanvallers via AD toegang kregen tot vertrouwelijke medische gegevens en aanzienlijke schade veroorzaakten. Aanvallers maken gebruik van technieken zoals 'Golden Ticket'-aanvallen, 'DCSync' en 'Kerberoasting' om toegang te krijgen tot gevoelige data zonder dat dit wordt opgemerkt door traditionele beveiligingstools. De complexiteit van hybride netwerkinfrastructuren maakt het steeds moeilijker om deze aanvallen te detecteren. Om AD effectief te beschermen, is een gelaagde beveiligingsaanpak noodzakelijk, inclusief strikte wachtwoordbeleid en voortdurende monitoring.

Google klaagt Chinese phishingplatform aan voor fraude via sms

Google heeft een rechtszaak aangespannen tegen het Chinese phishingplatform "Lighthouse", dat wereldwijd wordt gebruikt door cybercriminelen voor het stelen van creditcardinformatie via sms-phishingaanvallen, ook wel "smishing" genoemd. Het platform wordt beschuldigd van het vergemakkelijken van fraude via valse berichten die de Amerikaanse Postdienst (USPS) en tolbetalingssystemen zoals E-ZPass nabootsen. De rechtszaak, die gebaseerd is op federale racketeering- en fraudewetten, heeft als doel de website-infrastructuur van Lighthouse te sluiten, die volgens Google meer dan 1 miljoen slachtoffers heeft getroffen in 120 landen. De fraude heeft geleid tot de diefstal van tot wel 115 miljoen betaalkaarten in de VS tussen juli 2023 en oktober 2024. Google heeft ook steun uitgesproken voor nieuwe Amerikaanse wetgeving die consumenten moet beschermen tegen buitenlandse cybercriminaliteit.

North Sea Port Gent (B) stelt nieuw strategisch plan voor: havens beter beveiligen tegen drugs, cyberaanvallen en drones

North Sea Port heeft een strategisch plan gepresenteerd waarin de veiligheid van de havens van Gent, Terneuzen en Vlissingen centraal staat. Het doel is om tegen 2030 de fysieke en digitale beveiliging van de havens aanzienlijk te verbeteren. Er wordt gewerkt aan het uitbreiden van fysieke hekken van 3 naar 9 kilometer en er komen extra maatregelen om drones tegen te houden. De samenwerking met politie en justitie wordt versterkt, vooral om de invoer van drugs te bestrijden. Daarnaast is er aandacht voor cybersecurity, met een intensievere focus op bescherming tegen cyberaanvallen, in samenwerking met Nederlandse havens. Het plan benadrukt de noodzaak om de veiligheid te verhogen, gezien de groeiende risico's op zowel fysieke als digitale bedreigingen.