Cybercrimeinfo - cyberdreigingsanalyse (Openbare versie)

Europese defensieministers herbevestigen steun voor Oekraïne en versterken Europese verdediging

Op 14 november 2025 kwamen de defensieministers van Duitsland, Frankrijk, Groot-Brittannië, Italië en Polen samen in Berlijn om het eenjarig bestaan van de "Groep van Vijf" (GoF) te markeren. In een gezamenlijke verklaring herbevestigden zij hun commitment om Europa's defensiecapaciteiten te versterken en Oekraïne verder te ondersteunen in de strijd tegen de Russische agressie. Er werd een versnelling van de productiecapaciteit van de Europese defensie-industrie besproken, evenals samenwerking tussen Europese en Oekraïense bedrijven. De ministers benadrukten het belang van luchtverdedigingssystemen voor Oekraïne, vooral gezien de recente verhevigde Russische luchtaanvallen. Ze gaven ook prioriteit aan het versterken van de strijd tegen hybride dreigingen, zoals cyberaanvallen en desinformatie. De groep blijft zich inzetten voor continue militaire steun aan Oekraïne, waarbij de EU een cruciale rol speelt in de versterking van de Euro-Atlantische veiligheid.

Kritiek op Anthropic's claim van AI-geautomatiseerde cyberaanvallen door Chinese hackers

Anthropic heeft onlangs beweerd dat een door China gesponsorde dreigingsgroep, aangeduid als GTG-1002, een cyberespionage-operatie uitvoerde die grotendeels werd geautomatiseerd via misbruik van hun Claude Code AI-model. Volgens Anthropic was dit de eerste gedocumenteerde aanval waarbij AI vrijwel autonoom handelde in het uitvoeren van een cyberaanval. De aanval zou 30 doelwitten hebben getroffen, waaronder grote technologiebedrijven, financiële instellingen, chemische producenten en overheidsinstanties. Het AI-model zou de meeste fasen van de cyberaanval zelf hebben uitgevoerd, van het scannen van netwerken en het ontdekken van kwetsbaarheden, tot het exploiteren en verzamelen van inlichtingen.

De beweringen van Anthropic stuitten echter op veel scepsis binnen de cybersecuritygemeenschap. Veel onderzoekers beschouwen de rapporten als overdreven of zelfs verzonnen. Er werd kritiek geuit op het ontbreken van gedetailleerde technische informatie, zoals indicatoren van compromittering (IoC's), en de afwezigheid van concrete bewijzen voor de effectiviteit van de aanval. Desondanks stelde Anthropic dat de AI slechts in de beginfase werd ingegrepen door menselijke operators, en dat Claude in staat was om zelfstandig toegang te verkrijgen tot waardevolle doelwitten.

Deze aanval, die in september 2025 werd verstoord, werd gekarakteriseerd als een experiment waarbij AI werd ingezet voor penetratietests en exploitatie van kwetsbaarheden, met behulp van zowel open-source tools als een door AI gegenereerd aanvalsinfrastructuur. Hoewel de aanval slechts gedeeltelijk succesvol was, werd de operatie gepresenteerd als een belangrijke stap in de ontwikkeling van AI-gestuurde cyberaanvallen. De skeptici wijzen echter op de onrealistische verwachtingen van de huidige AI-technologieën en waarschuwen voor de overdrijving van de capaciteiten van AI in cyberaanvallen.

Noord-Koreaanse spionnen infiltreren Amerikaanse techbedrijven via valse identiteiten

Vijf personen, waaronder vier Amerikanen en één Oekraïner, hebben zich schuldig verklaard aan het faciliteren van Noord-Koreaanse spionageoperaties in de Verenigde Staten. Ze werkten mee aan een programma waarin Noord-Koreanen onder valse identiteit solliciteerden naar ICT-posities bij Amerikaanse techbedrijven, om zo toegang te verkrijgen tot bedrijfsnetwerken en systemen. Deze spionnen werkten op afstand, wat hun activiteiten moeilijker traceerbaar maakte.

Het Amerikaanse ministerie van Justitie heeft vastgesteld dat de spionnen zich vaak verhulden via tussenpersonen die internetverbindingen via Amerikaanse IP-adressen verschaften, evenals vervalste identiteitsdocumenten. Bovendien werden zogenaamde 'laptop-farms' ontdekt, ruimtes waar meerdere laptops op afstand werden aangestuurd vanuit Noord-Korea. Dit netwerk van spionnen werd ingezet om informatie te verzamelen en financiële middelen door te sluizen naar Noord-Korea.

Deze operatie is een voorbeeld van de toenemende dreiging van digitale infiltratie, waarbij technologiebedrijven onbewust betrokken raken bij cyberinlichtingenoperaties. Dit incident benadrukt de risico's van insider threats en de uitdagingen voor bedrijven om hun systemen te beschermen tegen onopgemerkte spionage. Het incident is onderdeel van een bredere trend waarin staten zich bedienen van geavanceerde digitale methoden om gevoelige informatie te verkrijgen.

Cisco Catalyst Center kwetsbaarheid stelt aanvallers in staat om beheerdersrechten te verkrijgen

Cybercrimeinfo - cyberdreigingsanalyse (Openbare versie)

Een ernstige beveiligingsfout in de Cisco Catalyst Center Virtual Appliance is ontdekt, die aanvallers met beperkte toegang in staat stelt om volledige beheerderscontrole over getroffen systemen te verkrijgen. De kwetsbaarheid, geïdentificeerd als CVE-2025-20341, heeft betrekking op virtuele appliances die draaien op VMware ESXi en heeft een hoge ernst, met een CVSS-score van 8.8. Dit vormt een aanzienlijke bedreiging voor organisaties die deze systemen gebruiken voor netwerkbeheer en -monitoring.

De kwetsbaarheid is het gevolg van inadequate invoervalidatie binnen het systeem. Wanneer gebruikers gegevens via webverzoeken indienen, controleert de software deze informatie niet op de juiste manier. Deze fout biedt aanvallers de mogelijkheid om speciaal ontworpen HTTP-verzoeken te sturen die het systeem misleiden en hen hogere rechten toekennen. Het risico is bijzonder groot omdat de aanval op afstand kan worden uitgevoerd, wat het gevaar voor blootgestelde systemen vergroot.

Wat deze kwetsbaarheid nog zorgwekkender maakt, is dat aanvallers slechts basis toegangsgegevens nodig hebben om deze te exploiteren. Iemand met alleen leesrechten, typisch toegewezen aan gebruikers die systeeminformatie moeten kunnen bekijken, kan deze fout gebruiken om zijn rechten te verhogen tot beheerdersniveau. Zodra aanvallers beheerdersrechten verkrijgen, kunnen ze nieuwe gebruikersaccounts aanmaken, systeeminstellingen aanpassen en andere ongeautoriseerde acties uitvoeren die de beveiliging van het gehele netwerk in gevaar brengen.

Cisco heeft bevestigd dat er geen openbare exploitatie van deze kwetsbaarheid is waargenomen, wat organisaties de kans geeft om hun systemen te patchen voordat grootschalige aanvallen beginnen. De kwetsbaarheid treft Cisco Catalyst Center Virtual Appliance versies 2.3.7.3-VA en latere versies. Cisco heeft versie 2.3.7.10-VA uitgebracht als de gepatchte versie die dit beveiligingsprobleem verhelpt. Organisaties die getroffen versies draaien, wordt aangeraden om onmiddellijk naar deze nieuwe versie te upgraden.

De kwetsbaarheid is alleen van toepassing op virtuele appliances die draaien op VMware ESXi. Hardware-appliances en AWS-gebaseerde virtuele appliances worden niet door dit probleem getroffen. Omdat er geen tijdelijke oplossingen beschikbaar zijn, is een software-update de enige effectieve manier om bescherming tegen deze kwetsbaarheid te bieden.

Phishingcampagne maakt misbruik van valse spamfiltermeldingen om e-mailinloggegevens te stelen

Een nieuwe phishingcampagne maakt gebruik van valse spamfiltermeldingen om gebruikers te misleiden en hun e-mailinloggegevens te stelen. De aanvallers versturen e-mails die beweren dat een organisatie zijn beveiligingssystemen heeft geüpgraded en dat sommige berichten niet in de inbox konden worden afgeleverd. De ontvangers worden aangemoedigd om op een link te klikken om de vastgehouden berichten in de inbox te verplaatsen. Deze link leidt echter naar een phishingwebsite die de inloggegevens van gebruikers probeert te stelen.

De e-mail is opvallend goed nagebootst, met ogenschijnlijk legitieme berichttitels en afleveringsrapporten die vertrouwd en onschuldig lijken. Daarnaast wordt er een afmeldlink toegevoegd om de e-mail authentieker te doen lijken. Zowel de knop als de afmeldlink leiden de slachtoffers via een omgeleide link naar de phishingpagina.

Wat deze aanval bijzonder maakt, is het gebruik van websockets voor het direct verzamelen van gegevens. Dit stelt de aanvallers in staat om de ingevoerde gegevens, zoals e-mailadressen en wachtwoorden, in realtime te ontvangen zonder dat de pagina hoeft te verversen. Het gebruik van websockets maakt het zelfs mogelijk om aanvullende verzoeken voor tweefactorauthenticatiecodes te sturen, waarmee aanvallers accounts met extra beveiligingslagen kunnen omzeilen.

Lumma Stealer gebruikt browserfingerprinting voor dataverzameling en stealthy C&C-communicatie

Lumma Stealer is een vorm van malware die via valse software-updates en gekraakte applicaties verspreidt. Deze malware is ontworpen om inloggegevens, betaalinformatie en cryptocurrency-walletdata van geïnfecteerde systemen te stelen. Het verspreidt zich voornamelijk via phishing-e-mails, schadelijke advertenties en gecompromitteerde websites. Lumma Stealer is bijzonder gevaarlijk doordat het gegevens verzamelt van meerdere webbrowsers, waaronder Chrome, Firefox, Edge en Brave. Het verzamelt wachtwoorden, ingevulde informatie, browsegeschiedenis en sessietokens. De malware maakt gebruik van browserfingerprinting om gedetailleerde apparaatinformatie te verzamelen en stelt zich in staat om verborgen communicatiekanalen met de command-and-control-servers op te zetten. Deze techniek helpt aanvallers om geïnfecteerde apparaten te volgen en communicatie te camoufleren als reguliere webverkeer. Geïnfecteerde systemen kunnen onopgemerkt

blijven totdat slachtoffers ongeautoriseerde transacties of accountinbreuken opmerken.

Akira ransomware: 250+ organisaties getroffen, 42 miljoen dollar geëist in losgeld

Akira ransomware is een van de meest actieve dreigingen die wereldwijd bedrijven treffen. Sinds maart 2023 heeft deze ransomware meer dan 250 organisaties in Noord-Amerika, Europa en Australië aangevallen, met een geschat losgeldbedrag van 244 miljoen dollar eind september 2025. De dreigingsactoren achter Akira worden in verband gebracht met de opgeheven Conti ransomwaregroep. Akira richt zich voornamelijk op kleine en middelgrote bedrijven in diverse sectoren, waaronder de maakindustrie, onderwijsinstellingen, informatie-technologie, gezondheidszorg en financiële dienstverlening.

De aanvallers verkrijgen toegang via virtuele privé-netwerken zonder geconfigureerde multi-factor authenticatie en maken gebruik van kwetsbaarheden in Cisco-producten. De groep past continu haar aanvalsmethoden aan, waarbij ze in 2025 gebruik maakt van verschillende encryptietools, waaronder de Megazord-encryptor, die een op Rust gebaseerde encryptie toevoegt. Akira gebruikt een double-extortion-model, waarbij naast het versleutelen van gegevens ook gedreigd wordt met de openbaarmaking van gevoelige informatie. De aanvallers zetten geavanceerde technieken in om toegang te behouden en verdere schade te veroorzaken.

Geavanceerde phishingkit gebruikt Telegram voor het verzamelen van inloggegevens en om automatische detectie te omzeilen

Een nieuwe phishingkit die onlangs werd ontdekt, heeft aangetoond hoe geavanceerd cybercriminelen hun methoden blijven verbeteren om gevoelige gegevens te stelen. Deze kit is ontworpen om de Italiaanse IT- en webserviceprovider Aruba S.p.A. te imiteren, een bedrijf dat meer dan 5,4 miljoen klanten bedient binnen de digitale infrastructuur van Italië. Door een dergelijke vertrouwde dienstverlener te targeten, kunnen aanvallers toegang krijgen tot kritieke bedrijfsmiddelen, waaronder gehoste websites, domeinbeheersystemen en e-mailsystemen. De phishingcampagne begint met spear-phishing-e-mails die urgentie creëren door te waarschuwen voor verlopen diensten of mislukte betalingen. De

berichten bevatten links naar valse inlogpagina's die sterk lijken op het officiële Aruba webmailportaal.

Wat deze aanval bijzonder slim maakt, is het gebruik van vooraf ingevulde inlog-URL's, waardoor het e-mailadres van het slachtoffer automatisch in het formulier wordt geplaatst. Dit vergroot de authenticiteit en maakt de slachtoffers minder wantrouwend, waardoor ze sneller hun wachtwoorden invoeren. Het framework achter deze aanval werkt verder met een vierfasenproces, waarbij eerst een CAPTCHA-uitdaging wordt gebruikt om bots te blokkeren, gevolgd door een valse inlogpagina, een nep-betalingspagina en uiteindelijk een frauduleuze 3D Secure-verificatiepagina. Alle gestolen gegevens worden via Telegram-kanalen direct naar de aanvallers verzonden, waardoor ze direct op de hoogte worden gehouden van elke nieuwe slachtofferinvoer. Nadat het proces is voltooid, worden de slachtoffers doorgestuurd naar de legitieme Aruba-website, waardoor ze onbewust blijven van de compromittering van hun gegevens.

Deze operatie benadrukt de groeiende trend van phishing-as-a-service, waarbij vooraf gebouwde kits de technische drempels verlagen en op industriële schaal bijdragen aan credential theft.

Formbook-malware verspreid via wapengebruikte zipbestanden en meerdere scripts

Formbook, een veelgebruikte malware, heeft opnieuw slachtoffers gemaakt door gebruik te maken van zipbestanden en meerdere scripts om beveiligingsmaatregelen te omzeilen. De aanvallen beginnen met phishing-e-mails die zipbestanden bevatten. Deze zipbestanden bevatten VBS-scripts die zich voordoen als betalingsbevestigingen. Wanneer een slachtoffer de bijlage opent, wordt het VBS-script geactiveerd, wat leidt tot een keten van gebeurtenissen die de malware uiteindelijk op het systeem van het slachtoffer installeert.

De multi-stadium-aanpak van de malware maakt het moeilijk om deze aanvallen te detecteren. Het VBS-script start een vertraging van negen seconden voordat het schadelijke acties onderneemt, waardoor detectiesystemen die zoeken naar onmiddellijke verdachte activiteiten worden omzeild. Vervolgens wordt een PowerShell-script gebruikt om een tweede payload van Google Drive te downloaden en op te slaan in de AppData-map van de gebruiker. Uiteindelijk wordt de Formbook-malware via msiexec.exe uitgevoerd, waarmee het verbinding maakt met een

command server om verdere instructies te ontvangen. De lage detectiegraad van de aanvallen benadrukt de effectiviteit van de gebruikte obfuscatietechnieken.

DigitStealer: Geavanceerde malware voor macOS ontwijkt detectie met multi-stage aanvallen

Een nieuwe malwarefamilie genaamd DigitStealer heeft macOS-systemen tot doel, met geavanceerde technieken om detectie te vermijden en gegevens te stelen. Deze informatie-stealer maakt gebruik van meerdere payloads om gevoelige gegevens te stelen, terwijl het minimaliseert hoe vaak het spoor achterlaat op geïnfecteerde systemen. De malware vermomt zich als legitieme software en maakt gebruik van slimme methoden om de beveiligingsmaatregelen van Apple te omzeilen. DigitStealer verspreidt zich via vervalste versies van populaire macOS-applicaties. De malware werd ontdekt in een niet-ondertekend diskimagebestand genaamd DynamicLake.dmg, dat zich voordeed als een legitiem hulpprogramma. Gebruikers worden misleid om een bestand genaamd “Drag Into Terminal.msi” uit te voeren, waardoor het infectieproces start.

Wat deze malware bijzonder maakt, is het gebruik van geavanceerde hardwarecontroles om te voorkomen dat het draait op virtuele machines of oudere Mac-computers. DigitStealer richt zich specifiek op de nieuwste Apple Silicon-systemen, met name M2-chips en hoger, en vermijdt Intel-gebaseerde Macs en zelfs M1-apparaten. De malware voert uitgebreide systeemcontroles uit voordat de hoofdpayload wordt uitgevoerd, zoals het controleren van de systeemlocatie en het zoeken naar specifieke kenmerken van Apple Silicon-processors. Alleen Mac-computers met deze geavanceerde ARM-processorfuncties worden besmet.

Na het doorlopen van deze controles downloadt DigitStealer vier afzonderlijke payloads van externe servers, met als doel het stelen van browserwachtwoorden, cryptocurrency wallets en het aanpassen van legitieme applicaties zoals Ledger Live. Door gebruik te maken van legitieme Cloudflare-diensten om de payloads te hosten, wordt het detecteren en blokkeren van de malware nog moeilijker.

Hackers misbruiken facturen om XWorm te verspreiden die inloggegevens steelt

Cybercriminelen gebruiken nep-facturen om XWorm, een remote access trojan (RAT), te verspreiden. Deze malware is in staat om inloggegevens, wachtwoorden en

gevoelige bestanden van besmette systemen te stelen. De aanval begint met een ogenschijnlijk onschuldige e-mail die een factuur of betalingsoverzicht bevat. Het bijgevoegde bestand is een Visual Basic Script (.vbs), dat, wanneer geopend, onmiddellijk kwaadaardige code uitvoert. Dit proces gebeurt op de achtergrond zonder waarschuwingen of meldingen, waardoor slachtoffers zich pas realiseren dat hun systeem is gecompromitteerd wanneer het te laat is.

XWorm biedt aanvallers volledige controle over de geïnfecteerde machines, waardoor ze toegang krijgen tot persoonlijke gegevens, het toekennen van administratorrechten mogelijk wordt, en de aanval kan worden uitgebreid met andere schadelijke software zoals ransomware. Het gebruik van verouderde technologie, zoals .vbs-bestanden, maakt deze aanvallen moeilijker te detecteren, aangezien de meeste moderne e-mailbeveiligingssystemen dergelijke bestandsformaten blokkeren. Toch slagen sommige aanvallen erin de filters te omzeilen en ernstige schade aan te richten.

Spam via TEA Protocol overspoelt npm, maar geen nieuwe wormdreiging

Een recente golf van spam die npm (Node Package Manager) overspoelt, heeft in de media onterecht de aanduiding "worm" gekregen. Dit betreft echter geen nieuwe vorm van malware, maar een voortzetting van de TEA Protocol spamcampagnes die al twee jaar actief zijn. Deze campagnes misbruiken open-source registratiesystemen om kunstmatig het aantal afhankelijkheden van spamprojecten te vergroten. Het doel is het verkrijgen van TEA-tokens via nepafhankelijkheden, wat het voor ontwikkelaars moeilijker maakt om betrouwbare code te vinden.

Hoewel de spam in sommige gevallen lijkt te repliceren, is er geen sprake van kwaadaardige zelf-replicatie, zoals bij wormen. De replicatie is het gevolg van een handmatig uitgevoerd publicatiescript dat geen automatische acties uitvoert bij de installatie van de pakketten. Deze campagne heeft geen directe schadelijke gevolgen voor de beveiliging van systemen, maar zorgt voor operationele verstoringen. De vervuiling van afhankelijkheidsnetwerken en het verbruik van middelen kunnen de efficiëntie van ontwikkelaars en tools die gebruik maken van npm negatief beïnvloeden. Het probleem heeft vooral impact op de infrastructuur van open-source projecten, met name in de mate van vervuiling van de registries en vertragingen bij het detecteren van echt schadelijke activiteiten.

Misbruik van het decennia-oude 'Finger' protocol in ClickFix malware-aanvallen

Cybercriminelen hebben het decennia-oude 'Finger' protocol opnieuw misbruikt in een serie aanvallen die nu bekendstaan als ClickFix-aanvallen. Het Finger protocol, oorspronkelijk ontwikkeld voor Unix- en Linux-systemen, wordt tegenwoordig zelden gebruikt, maar blijkt nog steeds actief in verschillende aanvallen. Het protocol wordt vaak gebruikt om commando's op afstand op Windows-systemen uit te voeren door kwaadaardige actoren.

Bij deze aanvallen wordt de 'finger' opdracht uitgevoerd op een kwetsbaar systeem, waarbij commando's worden opgehaald van een externe server. Deze commando's worden vervolgens via de Windows opdrachtprompt (cmd.exe) uitgevoerd. Recent werd een kwaadaardig batchbestand gedeeld, waarin het Finger protocol wordt gebruikt om commando's op te halen van een server. Wanneer het bestand wordt uitgevoerd, worden er scripts gedownload die uiteindelijk malware installeren op het systeem.

Een specifiek voorbeeld van deze aanvalsmethode is het misbruik van het Finger protocol via een vals CAPTCHA-venster. Gebruikers die in de verleiding komen om een vermeend beveiligingscommando in te voeren, lopen het risico dat hun systeem wordt geïnfecteerd. De malware die door deze aanvallen wordt geïnstalleerd, varieert, maar een veelvoorkomend type is een infostealer, die gevoelige informatie van het slachtoffer verzamelt en doorstuurt naar de aanvaller.

Het lijkt erop dat dit soort aanvallen specifiek gericht zijn op systemen die gevoelig zijn voor dit oude protocol, en hoewel de aanvallen tot nu toe voornamelijk door een enkele actor zijn uitgevoerd, wordt verwacht dat de dreiging zich kan uitbreiden. Als verdedigingsmaatregel kunnen organisaties het uitgaande verkeer naar poort 79, die door het Finger protocol wordt gebruikt, blokkeren om dergelijke aanvallen te voorkomen.

RondoDox benut onbeschermde XWiki-servers om meer apparaten aan zijn botnet toe te voegen

RondoDox, een botnet-malware, richt zich momenteel op onbeschermde XWiki-instanties die kwetsbaar zijn door de CVE-2025-24893-beveiligingsfout, een evaluatie-injectie die het mogelijk maakt voor aanvallers om op afstand willekeurige code uit te voeren. Deze kwetsbaarheid werd eind februari 2025 gepatcht in de versies XWiki 15.10.11, 16.4.1 en 16.5.0RC1, maar blijkt sindsdien in het wild te

worden misbruikt. Het werd aanvankelijk al in maart 2025 waargenomen, maar de aanvallen bereikten een hoogtepunt in oktober, toen de exploit in een keten van aanvallen werd ingezet om cryptocurrency-miners te installeren.

Op 3 november 2025 werd de eerste exploit door RondoDox geregistreerd, gevolgd door een toename van exploitatiepogingen. De aanvallen hebben een breed scala aan vectoren bereikt, waaronder DDoS-aanvallen via HTTP-, UDP- en TCP-protocollen. Dit wijst op de uitbreiding van RondoDox's bereik, waarbij apparaten wereldwijd worden ingepalmd voor cyberaanvallen. De VS Cybersecurity and Infrastructure Security Agency (CISA) heeft de kwetsbaarheid opgenomen in haar catalogus van bekende geëxploiteerde kwetsbaarheden, met een verplichting voor federale instanties om tegen 20 november mitigaties toe te passen.

Het blijft duidelijk dat een robuust patchbeheer essentieel is om dergelijke dreigingen tegen te gaan. RondoDox's exploitatie van deze kwetsbaarheid toont de noodzaak aan voor tijdige updates en bescherming tegen dergelijke aanvallen die de digitale veiligheid wereldwijd ondermijnen.

RONINGLOADER maakt gebruik van ondertekende stuurprogramma's om Defender uit te schakelen en EDR-tools te omzeilen

De afgelopen weken is er een nieuwe dreiging opgekomen die vooral gericht is op Chinese gebruikers, met de focus op het omzeilen van antivirusprogramma's en het uitschakelen van beveiligingshulpmiddelen op Windows-systemen. De malware, genaamd RONINGLOADER, maakt gebruik van slimme technieken om zijn werking te verbergen en verscheidene lagen van beveiliging te doorbreken. De infectie begint met nep-installateurs die zich voordoen als legitieme software, zoals Google Chrome of Microsoft Teams, en wanneer deze worden uitgevoerd, wordt de aanval in gang gezet.

Zodra RONINGLOADER zich op een systeem heeft gevestigd, probeert het meerdere beveiligingsmaatregelen te omzeilen. Dit gebeurt door het gebruik van een digitaal ondertekend stuurprogramma, dat oorspronkelijk bedoeld is voor legitiem gebruik maar in dit geval wordt misbruikt om Windows Defender en andere populaire Chinese beveiligingssoftware, zoals Qihoo 360, uit te schakelen. De malware gebruikt een techniek die door Windows wordt herkend als geldig, maar in werkelijkheid wordt het proces van beveiligingsschorsing uitgevoerd.

Een van de belangrijkste kenmerken van RONINGLOADER is het gebruik van een backupplan. Als een poging om de beveiliging uit te schakelen niet werkt, probeert de malware verschillende alternatieve methoden. De aanval maakt gebruik van een techniek die recentelijk in het openbaar werd gedocumenteerd, waarbij de malware de zogenaamde Protected Process Light (PPL) misbruikt om zich in te schrijven als een legitiem proces, maar uiteindelijk de beveiligingssoftware uitschakelt.

De dreiging die RONINGLOADER vormt, is dus een voorbeeld van hoe cybercriminelen hun methoden verfijnen, door gebruik te maken van steeds geavanceerdere technieken die de effectiviteit van traditionele beveiligingsmaatregelen ondermijnen. Cyberbeveiligingsexperts adviseren dan ook om waakzaam te blijven en proactief systemen te monitoren op ongebruikelijke activiteiten.

Vijf verdachten schuldig bevonden in Noord-Koreaanse spionageoperatie

Vijf individuen hebben zich schuldig verklaard voor hun rol in het helpen van Noord-Korea bij het infiltreren van Amerikaanse bedrijven, met als doel illegale inkomsten te genereren. De Verenigde Staten hebben aangekondigd dat de betrokkenen deel uitmaakten van een netwerk dat remote IT-werknemers rekruteerde en fraude pleegde. Het doel van de operatie was om de Noord-Koreaanse regering van fondsen te voorzien, via illegale activiteiten zoals cryptocurrency-diefstal en het opzetten van valse identiteiten voor werknemers in Amerikaanse bedrijven.

De vijf verdachten, waaronder vier Amerikanen en één Oekraïner, gebruikten gestolen of valse identiteiten om Noord-Koreaanse agenten in te huren bij 136 Amerikaanse bedrijven. Het proces leverde meer dan 2,2 miljoen dollar op voor het Noord-Koreaanse regime. De verdachte Oleksandr Didenko, die betrokken was bij de verkoop van gestolen Amerikaanse identiteiten, stemde ermee in om 570.000 dollar in fiatvaluta en 830.000 dollar aan cryptocurrency in beslag te nemen. Daarnaast zijn er juridische stappen ondernomen om in totaal 15 miljoen dollar aan gestolen cryptocurrency, die afkomstig is van hacks in 2023, in beslag te nemen. Deze hacks, uitgevoerd door de APT38-groep, richtten zich op cryptobeurzen in Panama, Estland en de Seychellen, met als resultaat de diefstal van 382 miljoen dollar.

Logitech bevestigt datalek na Clop-extortieaanval

Logitech heeft bevestigd dat het slachtoffer is geworden van een datalek, veroorzaakt door een cyberaanval die werd opgeëist door de Clop-extortiegroep. Het Zwitserse technologiebedrijf, bekend van zijn hardware en softwareproducten, meldde het incident aan de Amerikaanse Securities and Exchange Commission (SEC). De aanval vond plaats via een kwetsbaarheid in de Oracle E-Business Suite, die eerder in juli werd misbruikt door de aanvallers.

Logitech verklaarde dat het datalek geen invloed heeft gehad op hun producten, bedrijfsvoering of productieprocessen. Gevoelige gegevens zoals nationale identificatienummers of creditcardinformatie waren niet aangetast, aangezien deze gegevens niet waren opgeslagen in de getroffen systemen. De gestolen informatie zou beperkte gegevens van werknemers, consumenten, klanten en leveranciers omvatten.

De aanval werd mogelijk gemaakt door een zero-day kwetsbaarheid die snel werd gepatcht zodra de oplossing beschikbaar was. Clop heeft bijna 1,8 TB aan gegevens gelekt, en dit komt ko

rt nadat het bedrijf in verband werd gebracht met de exploitatie van een Oracle-kwetsbaarheid. Logitech werkt samen met externe cybersecurity-experts om het incident te onderzoeken.

AI-technologie maakt stemmen nauwelijks meer van menselijke te onderscheiden, wat betekent dit voor de beveiliging?

De recente vooruitgang in kunstmatige intelligentie (AI) heeft geleid tot de ontwikkeling van technologie die in staat is om stemmen en muziek te genereren die niet van echte mensen te onderscheiden zijn. Dit opent nieuwe mogelijkheden, maar ook risico’s. Onderzoek van Deezer en Ipsos toont aan dat 97 procent van de mensen het niet doorheeft wanneer muziek door AI is gecomponeerd. Bovendien onthulde een studie van de Queen Mary University in Londen dat meer dan de helft van de deelnemers moeite had om te herkennen of een stem afkomstig was van een mens of van AI.

Voor cybercriminelen biedt deze technologie nieuwe kansen om digitale misleiding en identiteitsfraude te plegen. Het gebruik van AI om stemmen van beroemdheden of andere publieke figuren na te maken, kan bijvoorbeeld worden ingezet voor oplichting, zoals het afnemen van gevoelige informatie of het uitvoeren van valse aanvragen. De technologie achter deepfake-video’s en -audio kan ook worden

ingezet voor politieke manipulatie, financiële fraude of het uitvoeren van social engineering-aanvallen.

Tegelijkertijd zien we dat sommige beroemdheden, zoals de acteurs Michael Caine en Matthew McConaughey, hun stemmen beschikbaar stellen voor commerciële toepassingen via AI, wat de vraag oproept hoe we als samenleving omgaan met de ethische en juridische implicaties van dergelijke technologieën. In de context van cybercrime en digitale veiligheid is het van belang dat bedrijven en individuen zich bewust zijn van de potentie van AI om zowel beveiligingsrisico's als kansen te creëren voor cybercriminelen.

Als deze technologie onbeheerd wordt gebruikt, kunnen de gevolgen verstrekkend zijn voor privacy en digitale veiligheid. Het is cruciaal dat er strikte regels en technologieën worden ontwikkeld om misbruik van AI te voorkomen en om gebruikers beter te beschermen tegen de gevaren van valse digitale identiteiten.

Jaguar Land Rover verliest $220 miljoen door cyberaanval

Jaguar Land Rover (JLR) heeft in haar financiële resultaten voor het derde kwartaal van 2025 bekendgemaakt dat de recente cyberaanval haar ruim $220 miljoen heeft gekost. De aanval, die op 2 september werd aangekondigd, dwong het bedrijf om de productie op belangrijke fabrieken tijdelijk stop te zetten. Werknemers moesten naar huis gestuurd worden, en de productie werd wekenlang verstoord. Tijdens de aanval werd gevoelige data gestolen, wat de cybercriminaliteitsgroep Scattered Lapsus$ Hunters via Telegram claimde.

De gevolgen van de cyberaanval waren niet alleen financieel ingrijpend, maar hadden ook een sterke invloed op de marktpositie van JLR en veroorzaakten ernstige liquiditeitsproblemen bij sommige van hun leveranciers. Op 29 september tussenbeide de Britse overheid door een leninggarantie van £1,5 miljard goed te keuren, waarmee de toeleveringsketen van het bedrijf hersteld kon worden en de productie op 8 oktober weer geleidelijk werd hervat.

De impact op de winst was groot. Het bedrijf meldde een verlies vóór belasting van £485 miljoen voor het tweede kwartaal, en £134 miljoen voor de eerste helft van het jaar, tegenover een winst van £398 miljoen en £1,1 miljard in dezelfde perioden van het voorgaande jaar. JLR gaf aan dat de afname in winst vooral te wijten was aan de cyberaanval, de aanhoudende effecten van Amerikaanse tarieven, verminderde volumes en verhoogde kosten.

Ondanks deze ernstige gevolgen voor de financiële prestaties, benadrukte JLR dat de bedrijfsvoering inmiddels gestabiliseerd is. Logistiek, groothandel en leveranciersfinanciering zijn volledig hersteld, en het bedrijf blijft haar geplande investeringen van £18 miljard voor de komende vijf jaar handhaven.

Massale verkoop van 1.200 FortiGate VPN-netwerkinloggegevens op het darkweb

Op 16 november 2025 werd melding gemaakt van de verkoop van 1.200 inloggegevens voor FortiGate VPN-netwerken op het darkweb. Deze gegevens, afkomstig uit eerdere cyberinbraken, bieden toegang tot beveiligde netwerken en vormen een aanzienlijk risico voor de getroffen organisaties. FortiGate is een veelgebruikte VPN-oplossing, die door bedrijven en overheidsinstellingen wordt ingezet om de netwerken te beveiligen. De verhandeling van dergelijke inloggegevens benadrukt de gevaren van datalekken en de handel in gevoelige informatie op illegale marktplaatsen.

De beschikbaarheid van deze inloggegevens op het darkweb vergroot de kans op misbruik door kwaadwillende actoren, die deze toegang kunnen gebruiken voor ransomware-aanvallen, digitale spionage of andere vormen van cybercriminaliteit. Dit incident onderstreept de voortdurende dreiging van gegevensdiefstal en de impact op de cyberbeveiliging van organisaties.

Kabinet stelt uitzonderingen voor acceptatieplicht contant geld voor

Het demissionaire kabinet heeft aangekondigd verschillende uitzonderingen te maken voor de wet die de acceptatieplicht van contant geld regelt. De wet zou in 2027 van kracht worden, maar het kabinet wil contante betalingen tussen 22.00 en 06.00 uur uitsluiten, evenals betalingen bij onbemande locaties zoals tankstations en in het openbaar vervoer. De wet is onderdeel van bredere inspanningen om witwaspraktijken te bestrijden. Kleine ondernemers met minder dan vier werknemers kunnen, vanwege veiligheidsrisico's, ook weigeren contant geld te accepteren.

De wetgeving heeft implicaties voor de digitale en fysieke veiligheid, aangezien sommige uitzonderingen kunnen leiden tot meer gebruik van alternatieve betaalmethoden zoals digitale betalingen, die op hun beurt cyberdreigingen kunnen versterken. Cybercriminelen kunnen mogelijk profiteren van de uitfasering van contant geld om meer geavanceerde digitale aanvallen uit te voeren, zoals phishing

en ransomware-aanvallen gericht op elektronische betalingen. Het wetsvoorstel wordt momenteel besproken en kan in de toekomst invloed hebben op de manier waarop consumenten en bedrijven met digitale en fysieke betalingen omgaan.

Kamervragen over aangepast Europees voorstel voor chatcontrole

Er zijn Kamervragen gesteld in de Tweede Kamer over het aangepaste voorstel van de Europese Unie met betrekking tot chatcontrole. Het voorstel, afkomstig van de Deense EU-voorzitterschap, kan chatdiensten en andere aanbieders verplichten om de inhoud van berichten te monitoren. Dit is een opvolging van een eerder voorstel dat wegens gebrek aan steun onder EU-lidstaten niet werd aangenomen. Het aangepaste voorstel laat de mogelijkheid voor chatcontrole echter bestaan, wat leidt tot bezorgdheid over de ondermijning van end-to-end encryptie en de mogelijke schending van privacy en burgerrechten. Critici wijzen op de negatieve effecten van dit voorstel op de bescherming van anonimiteit, met name voor journalisten, activisten en hulpzoekenden.

In reactie op het voorstel heeft GroenLinks-PvdA-Kamerlid Kathmann Kamervragen gesteld aan demissionair minister Van Oosten van Justitie en Veiligheid. De vragen richten zich op het waarborgen van privacy en het voorkomen van verplichtingen voor techbedrijven om materiaal te detecteren. Ook wordt gevraagd of Nederland kan instemmen met het voorstel zonder dat chatcontrole volledig wordt uitgesloten. De antwoorden van de minister worden binnen drie weken verwacht.