Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC Maandmonitor

april 2021

Maandelijks analyseert het NCSC de belangrijkste ontwikkelingen op het gebied van digitale veiligheid. Dit document beschrijft deze ontwikkelingen voor de maand april 2021. Naast de feitelijke ontwikkelingen zijn in dit document ook links naar de bronnen [🖱] en commentaren van het NCSC opgenomen.

Actief misbruik van VPN-kwetsbaarheden door actoren

De afgelopen maand gingen meerdere berichten over actief misbruik van kwetsbaarheden in VPN-systemen. Op 20 april 2021 publiceerde Pulse Secure in een blogpost dat er actief misbruik wordt gemaakt van kwetsbaarheden in de Pulse Connect Secure Appliance. [🖱1] Ook de Amerikaanse Cybersecurity and Infrastructure Security Agency (CISA) laat weten dat er actief misbruik wordt gemaakt van deze kwetsbaarheden. [🖱2]
Het gaat om vier kwetsbaarheden, waaronder voor drie oudere waar in 2019 en 2020 beveiligingsupdates voor zijn uitgebracht. Het heeft hier NCSC destijds beveiligingsadviezen voor geschreven. [🖱3][🖱4][🖱5] De vierde kwetsbaarheid is nieuw en heeft als kenmerk CVE-2021-22893. Dit was een zero-day kwetsbaarheid, waar in eerste instantie geen oplossing voor was. Begin mei 2021 is voor deze kwetsbaarheid een beveiligingsupdate uitgebracht. Het NCSC heeft voor deze Pulse Secure-kwetsbaarheden een "high/high" beveiligingsadvies gepubliceerd. Dit betekent dat de kans en de potentiële schade als hoog worden ingeschat. [🖱6]
Ook is er deze maand door CISA, NSA en FBI een gezamenlijk beveiligingsadvies uitgebracht waarin zij claimen dat een Russische actor misbruik maakt van vijf kwetsbaarheden in verschillende producten, waaronder een aantal met een VPN-component [🖱7]:

- CVE-2018-13379, in FortiGate SSL VPN [🖱8];
- CVE-2019-11510, in Pulse Connect Secure (PCS) [🖱9];
- CVE-2019-19781, in Citrix software [🖱10];
- CVE-2020-4006, in VMware software [🖱11];
- CVE-2019-9670, in Zimbra Collaboration Suite [🖱12];

Daarnaast meldt beveiligingsbedrijf FireEye dat er actief misbruik wordt gemaakt van een kwetsbaarheid in de SonicWall-VPN SMA100. Door middel van SQL-injectie kan een ongeauthenticeerde kwaadwillende op afstand toegang tot inloggegevens krijgen en het kwetsbare VPN-systeem overnemen. Ook dit betrof een zero-day kwetsbaarheid. Volgens het beveiligingsbedrijf is er actief misbruik van de kwetsbaarheid gemaakt, nog voordat een beveiligingsupdate beschikbaar was. De aanvallen worden toegeschreven aan criminelen. [🖱13] [🖱14] Het NCSC heeft in februari een beveiligingsadvies gepubliceerd voor de kwetsbaarheid in SonicWall-VPN SMA100. [🖱15]

- Bovenstaande voorbeelden laten zien dat VPN-systemen een geliefd doelwit blijven van zowel statelijke actoren als criminelen. De AIVD schrijft in het jaarverslag 2020 dat statelijke actoren aanzienlijk meer aanvalsmogelijkheden hebben voor digitale spionage omdat mensen veel meer thuiswerken. [🖱16] Hierdoor zijn organisaties afhankelijker van software waarmee op afstand inloggen op het kantoornetwerk mogelijk is. VPN-systemen voor thuiswerkers zijn met het internet verbonden en hebben vaak vergaande toegang tot het netwerk. Doordat communicatie met deze apparaten via het internet mogelijk is, zijn ze ook makkelijker te misbruiken. [🖱17] Indien een kwaadwillende succesvol een VPN-systeem weet te compromitteren, kan dit een grote impact hebben op de betrouwbaarheid van de IT-infrastructuur.
- Het NCSC heeft in mei 2020 een bericht gepubliceerd over statelijke actoren die actief scannen naar VPN-kwetsbaarheden. [🖱18] Het advies in dit bericht blijft van toepassing: zorg ervoor dat u de meest recente beveiligingsupdates uitvoert, overweeg implementatie van tweefactor-authenticatie en regel logging en monitoring in.
- Het NCSC verwijst daarnaast ook naar het stappenplan dat de AIVD op haar website heeft geplaatst om misbruik van VPN-verbindingen en mailservers te voorkomen. [🖱19]

Sociale media door statelijke actoren ingezet als aanvalsvector

Afgelopen maand kwamen diverse campagnes in het nieuws over het misbruiken van sociale media door kwaadwillenden om gericht informatie te verkrijgen. [🖱20] Het inzetten van sociale media voor onder andere spionagedoeleinden is niet nieuw en gebeurt op diverse wijzen. Zoals het aanmaken van nepprofielen [🖱21], malwarebesmetting en het verzamelen van persoonsgegevens en/of misbruiken van (gelekte) accountgegevens. [🖱22]
De nepprofielen worden bijvoorbeeld gebruikt om het

vertrouwen te winnen van personen binnen een specifieke sector/ branche of bedrijf of met een specifieke functie om zo gericht informatie te kunnen inwinnen. [23]
Een andere werkwijze is dat het nepaccount een zogenaamde recruiter betreft. [24] Dit soort nepaccounts worden onder andere gebruikt om zogenaamd diensten te verkopen aan specifieke doelgroepen die daar mogelijk geïnteresseerd in zijn. In werkelijkheid willen zij informatie ontfutselen van het slachtoffer door via een chatfunctie vragen te stellen of het apparaat van het slachtoffer te infecteren. Daarnaast kan een recruiter zogenaamd inspelen op de carrière van het doelwit door een andere functie met goed salaris aan te bieden. Om dit kracht bij te zetten, stuurt de aanvaller een malafide link naar een vacaturesite of bedrijfswebsite (van een niet bestaand bedrijf) of een besmette bijlage met de zogenaamde vacaturetekst. [25] Indien de geïnteresseerde op de link klikt of het bestand opent, wordt het apparaat geïnfecteerd met malware. Dit kan een backdoor of Remote Access Trojan (RAT) zijn zodat toegang op afstand wordt verkregen tot het apparaat en informatie kan worden gestolen of kan worden ingezet om te spioneren (bijvoorbeeld middels het heimelijk inschakelen van de camera en/of microfoon). [26]

- Het gebruik van sociale media is gedurende de COVID-19 pandemie toegenomen. Veel Nederlanders hebben een account op een of meerdere sociale mediaplatformen. [27] Deze accounts bevatten vaak een (gebruikers)naam, e-mailadres of meer gegevens en voorzien daarmee kwaadwillenden van gratis informatie. Ook kunnen deze gegevens ongewenst in een database voorkomen na bijvoorbeeld een datalek. Controleer op https://haveibeenpwned.com/ of uw e-mail of telefoonnummer onderdeel uitmaakt van een gelekte dataset.
- Diverse internationale overheidsinstanties, onder andere Amerikaanse, Australische en Britse, zijn eind vorig jaar al een bewustzijnscampagne begonnen. [28] [29] [30]
- Bescherm zo goed mogelijk uw (persoonlijk herleidbare) gegevens online en wees terughoudend met het delen van deze (persoonlijke) informatie. [31]

FluBot-smishing-campagne ook in Nederland waargenomen

Het Britse NCSC-UK en het Duitse BSI waarschuwden deze maand voor sms-phishing-campagnes die resulteren in een infectie met de FluBot-malware. [32] [33] De sms-berichten lijken afkomstig van vervoersbedrijven zoals DHL of FedEx. In de sms-berichten wordt de telefooneigenaar gevraagd een app te installeren. Wanneer de gebruiker dit doet resulteert dit in een infectie met de FluBot-malware. FluBot gedraagt zich als spyware en kan onder andere via SMS spam-berichten versturen en inloggegevens stelen. FluBot verspreidt zich na infectie verder door nieuwe SMS-berichten te versturen naar het adresboek van het slachtoffer. [34]
De huidige campagnes richten zich op Android-telefoons, vooralsnog zijn geen campagnes gericht op iPhones waargenomen. Volgens onder andere Vodafone UK worden de sms-berichten steeds vaker waargenomen in een groot aantal landen. [35] [36] Ook het NCSC heeft dit jaar meldingen ontvangen van Flubot-infecties.

- Phishing via sms ('smishing') is geen nieuw fenomeen. Ook platformen als WhatsApp, Facebook en LinkedIn worden misbruikt voor phishing. Dat bleek ook deze maand in diverse phishing-campagnes. [37] [38]
- De FluBot-malware verstuurt na installatie nieuwe phishing-berichten naar de contactlijst van het slachtoffer. Daarom was deze malware de afgelopen maand erg zichtbaar, met name bij telecomproviders.
- Het NCSC adviseert om nieuwe apps voor uw mobiele apparaat altijd aan te schaffen via officiële distributiekanalen van leveranciers, de zogenaamde 'appstores'. Zie ook de beveiligingsrichtlijnen voor mobiele apparaten. [39]
- Bezoek altijd de website van de vervoerder, wanneer een pakket wordt verwacht, en controleer dit niet via de aangeboden link in tekstberichten.

Overig nieuws Nederland

NCSC mag dreigingsinformatie met Connect2Trust gaan delen [40] ■ Veel mis in Nederlandse ict-beveiliging, zelfs geen verweer tegen simpele hacks [41] ■ Politie ziet meldingen van cybercrime in eerste kwartaal verdubbelen [42] ■ Data ICT-bedrijf Managed IT was versleuteld met Bitlocker en losgeld is betaald [43] ■ Bijna honderd notariskantoren geraakt door hack [44] ■ EU onderzoekt cyberaanval op aantal van haar instellingen [45] ■ Waternet onder verscherpt toezicht wegens onvoldoende grip op cybersecurity [46] ■ Politie en OM: meer investeren in cyberweerbaarheid Nederland [47] ■ Utrecht slaat schertsfiguur met informatiebeveiliging [48] ■ Low-code software helpt zeehavens bij gevaar [49] ■ CSR adviseert €833 miljoen voor een integrale aanpak voor cyberweerbaarheid [50] ■ Politie neemt in onderzoek naar phishing 300.000 euro in beslag [51] ■ Minister wil dat openbaar bestuur permanent digitaal kan vergaderen [52] ■ AIVD: Citrix-lek vorig jaar op grote schaal door Rusland misbruikt [53]