TLP:WHITE

Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC Maandmonitor

mei 2021

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

Update: Grote toename FluBot-infecties waargenomen in Nederland

In de maandmonitor van april 2021 waarschuwde het NCSC al dat infecties met de FluBot-malware waren waargenomen in Nederland. Deze maand is het aantal waarnemingen in Nederland significant toegenomen. Dit is het resultaat van een smishing (sms-phishing)-campagne gericht op Nederlandse Android-gebruikers. Verschillende instanties hebben daarom deze maand waarschuwingen uitgegeven. [🖱1] [🖱2] [🖱3] [🖱4] Ook verschenen er berichten in de Nederlandse media. [🖱5] [🖱6] Beveiligingsonderzoekers hebben ontdekt dat in dezelfde campagne die FluBot verspreidt ook de 'Anatsa'-malware wordt verspreid. [🖱7] Anatsa is een soortgelijke malware als FluBot, een soort spyware die onder andere inloggegevens kan stelen, maar heeft volgens onderzoekers meer functionaliteiten. Daarnaast richt Anatsa zich specifiek op gebruikers van apps van Nederlandse banken. Dat laatste is voor zover bekend niet het geval bij FluBot.

- Zie de adviezen en duiding die zijn gegeven in de maandmonitor van april 2021, deze zijn nog steeds actueel.
- Een toevoeging hierop is dat er mogelijke detectiemaatregelen voor FluBot beschikbaar zijn. [🖱8]

Belgische ministerie van Binnenlandse Zaken slachtoffer van digitale aanval

De Belgische Federale Overheidsdienst (Ministerie) van Binnenlandse Zaken is slachtoffer geworden van een digitale aanval. [🖱9] In maart 2021 werd bekend dat de actor HAFNIUM misbruik maakte van kwetsbaarheden in Microsoft Exchange. Naar aanleiding van deze berichten is het Centrum voor Cybersecurity België (CCB) een onderzoek gestart. Het NCSC heeft voor deze kwetsbaarheden ook een beveiligingsadvies uitgebracht. [🖱10]
Uit het onderzoek van CCB is gebleken dat inderdaad sprake was van geïnstalleerde backdoors op het netwerk van het ministerie. Deze zijn door het CCB verwijderd en de beschikbare Microsoft updates zijn uitgevoerd. Het CCB heeft vervolgens aanvullende monitoring uitgevoerd. Hieruit bleek dat vanaf april 2019 verdachte handelingen op het netwerk van het ministerie heeft plaatsgevonden. Na deze bevinding is de kwetsbaarheid in het netwerk verholpen, is belangrijke gevoelige informatie veiliggesteld en is gestart met het opschonen van de systemen. Het CCB geeft aan dat het om een zeer complexe en geavanceerde aanval gaat en dat het vermoedelijk voor spionagedoeleinden is geweest. [🖱11]

- Het getroffen ministerie is de centrale schakel in de beveiliging en besturing van België, onder meer de politiediensten en crisisbeheer vallen onder dit ministerie. Dat een dergelijk ministerie slachtoffer is van een aanval heeft potentieel grote gevolgen.
- Microsoft heeft in 2021 aangegeven dat de, door hen zo genoemde, statelijke actor HAFNIUM misbruik maakte van de Microsoft Exchange-kwetsbaarheden. [🖱12] [🖱13]

Ransomware raakt het fysieke domein

In de maand mei zijn er verschillende berichten geweest over ransomware-aanvallen die grote impact hebben gehad op het fysieke domein. Op 7 mei 2021 is het oliepijplijnbedrijf Colonial Pipeline slachtoffer geworden van een ransomware-aanval. Ondanks dat bij deze aanval alleen het IT-netwerk en niet het OT-netwerk is geraakt, heeft Colonial Pipeline toch besloten om de operationele processen ook stop te zetten om mogelijke verdere verspreiding van de ransomware te voorkomen. Dit heeft grote gevolgen gehad voor de toelevering van brandstof aan de oostkust van de Verenigde Staten. En had ook indirecte gevolgen op de maatschappij zoals de onrust die ontstond en mensen die brandstof gingen hamsteren. Na zes dagen zijn de operationele processen weer opgestart. [🖱14] [🖱15] De FBI heeft in een persbericht bevestigd dat het de ransomware Darkside betreft. [🖱16]
De Ierse publieke gezondheidsdienst (HSE) is ook geraakt door een ransomware-aanval de afgelopen maand. Ook hier werd besloten om de IT-systemen offline te halen om verdere verspreiding te voorkomen. Dit heeft gevolgen gehad voor de zorgverlening aan patiënten, verschillende ziekenhuizen en instellingen. Via Twitter werd gemeld dat ofwel vertraging is opgetreden of dat afspraken zijn geannuleerd. [🖱17] [🖱18] [🖱19] [🖱20] De ransomware betreft de Conti-ransomware. Op het moment van schrijven heeft de Ierse HSE nog niet de controle terug over de systemen. [🖱21]

Zowel de Darkside-ransomware als Conti-ransomware wordt aangeboden als ransomware-as-a-service. [22] [23] Dit betekent dat een kwaadwillende de ransomware tegen betaling kan inzetten en dat de ontwikkelaars van de ransomware meedelen in de winst die gemaakt wordt. Vaak probeert een kwaadwillende extra druk te zetten op het slachtoffer om tot betaling over te gaan, door te dreigen de gestolen, gevoelige data te publiceren. In het geval van de aanval op de Ierse HSE is er ook daadwerkelijk gevoelige data gepubliceerd. [24]

- Beide incidenten demonstreren hoe ernstig de gevolgen kunnen zijn van een ransomware-aanval. Niet alleen op de korte termijn, zoals de uitval van diensten, maar ook op de lange termijn zullen de gevolgen merkbaar zijn. Denk hierbij aan de brandstofprijzen in de VS en het ontstaan van langere wachttijden in de zorg omdat geannuleerde afspraken opnieuw ingepland moeten worden.
- In de maandmonitor van februari dit jaar heeft het NCSC reeds geschreven over de toename in ransomware-aanvallen, zowel in Nederland als internationaal. Een aanval met grote gevolgen zoals in de VS en Ierland is ook in Nederland voorstelbaar. Het blijft van belang dat organisaties zich bewust zijn van de keteneffecten van ransomware-aanvallen en de gevolgen die de afhankelijkheid van IT-systemen teweeg brengen.
- Het NCSC heeft vorig jaar een factsheet over ransomware gepubliceerd met onder meer maatregelen om ransomware-aanvallen te voorkomen en te beperken. [25]

Opnieuw kwetsbaarheden ontdekt in draadloze protocollen

In mei zijn meerdere kwetsbaarheden gepubliceerd in de draadloze protocollen voor Wi-Fi en bluetooth. Bij Wi-Fi gaat het om zowel ontwerpfouten in het protocol als implementatiefouten in Wi-Fi-apparatuur. [26] Deze fouten zitten in de functionaliteit voor het bundelen en opsplitsen van pakketten (waarmee de snelheid en/of de stabiliteit van een draadloze verbinding kan worden verbeterd). De impact van deze fouten is afhankelijk van het type apparaat en de gebruikte instellingen. Zo kunnen aanvallers in voorkomende gevallen data injecteren in het verkeer tussen access points en een apparaat. [27] Dit maakt het voor een kwaadwillende mogelijk om bijvoorbeeld de instellingen van een DNS-server zodanig aan te passen waardoor gegevens worden omgeleid. Inmiddels heeft de beveiligingsonderzoeker die de fouten heeft ontdekt ook testtools beschikbaar gesteld. [28] Daarnaast hebben verschillende leveranciers patches beschikbaar gesteld voor deze kwetsbaarheden, inclusief benodigde mitigerende maatregelen voor de ontwerpfouten.
Bij bluetooth gaat het om ontwerpfouten in de bluetooth Core- en Bluetooth Mesh-specificaties. [29] Hierdoor kan een aanvaller onder andere een geauthentiseerd apparaat emuleren. Ook voor deze ontwerpfouten hebben verschillende leveranciers inmiddels patches beschikbaar gesteld.

- Zowel bluetooth als Wi-Fi hebben eerder te maken gehad met kwetsbaarheden in de protocollen. Dit benadrukt het belang van aandacht voor security bij de totstandkoming van (netwerk)protocollen. Naast het voorkomen van complexiteit [30], kunnen aanvullende maatregelen getroffen worden zoals: externe validatie, het gebruik van raamwerken [31] en het toepassen van methoden om correctheid te valideren. [32] [33] Deze maatregelen worden niet overal toegepast.
- Naast ontwerpfouten in protocollen, kunnen er ook fouten gemaakt worden bij de implementatie van de protocollen. Protocolontwerpers en programmeurs kunnen de kans op fouten verkleinen door een aantal maatregelen te nemen. [34] [35] [36] [37] [38] [39] Om misbruik van kwetsbaarheden te voorkomen dienen gebruikers van (draadloze) apparatuur updates direct te installeren wanneer deze beschikbaar worden gesteld.
- VPN-oplossingen, https, en andere vormen van (end-to-end) versleuteling kunnen de impact van kwetsbaarheden in onderliggende protocollagen mitigeren.

Overig nieuws Nederland

CSR: Nederland te afhankelijk van grote buitenlandse techbedrijven [40] ■ ACM begint verkennend onderzoek naar clouddiensten [41] ■ Rekenkamer: informatiebeveiliging Rijksoverheid nog niet op orde [42] ■ Huawei bevestigt in Nederland geen core-technologie voor 5G-netwerken te leveren [43] ■ Minder verdachten wegens cybercrime veroordeeld tot gevangenisstraf [44] ■ RDC weet niet hoe data miljoenen Nederlandse autobezitters is gestolen [45] ■ Hoger onderwijs wordt aangesloten op Security Operations Center [46] ■ Ministerie van Landbouw: toename van datalekken door thuiswerken [47] ■ Grapperhaus: aanpak van hostingbedrijven die misdaad faciliteren complex [48] ■ VWS in actie tegen datalek door verlopen domein [49] ■ Elektriciteitsproducenten moeten vanaf 1 juni verplicht aan Wbni voldoen [50] ■ Veel gemeenten niet voorbereid op cyberaanvallen [51]