TLP:WHITE

Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC Maandmonitor

juli 2021

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

Nieuwe Windows-kwetsbaarheden, beveiligingsmaatregelen en updates

In juli werden verschillende nieuwe kwetsbaarheden in Microsoft Windows bekend en soms ook al misbruikt. Zo vormden verschillende kwetsbaarheden een 'PrintNightmare'. [🖱1] [🖱2] [🖱3] Deze zijn ontdekt in de 'Print spooler service'. Dit is een proces binnen Windows dat gebruikt wordt voor printfunctionaliteit. Microsoft adviseert in bepaalde gevallen deze functionaliteit uit te schakelen om het aanvalsoppervlak te verkleinen. [🖱4] Een andere print-gerelateerde kwetsbaarheid bevindt zich in de 'Point and Print'-functionaliteit van Windows. Met deze functionaliteit kunnen gebruikers zonder administrator-rechten Windows-drivers installeren. Wanneer een systeem verbinding maakt met een malafide printer kan een aanvaller door middel van de kwetsbaarheid willekeurige code uitvoeren. [🖱5]

Ook werd de PetitPotam-aanvalsmethode bekend gemaakt. Deze aanval richt zich op Microsofts NTLM-authenticatiesysteem. PetitPotam is een NTLM-relay-aanval waarbij een aanvaller een systeem forceert door een malafide server te authentiseren en authenticatiegegevens door te geven. NTLM is een ouder authenticatieprotocol, waarvan Microsoft adviseert het gebruik zoveel mogelijk te beperken (een veiliger alternatief is Kerberos). [🖱6]

Tot slot werd bekend dat het Security Accountmanager (SAM)-bestand in Windows voor lokale gebruikers leesbaar is. Hierin wordt gevoelige informatie opgeslagen zoals wachtwoordinformatie. De kwetsbaarheid staat bekend als de 'HiveNightmare'- of 'SeriousSAM'-kwetsbaarheid. [🖱7]

- *Naast het tijdig installeren van patches is het ook van belang om beveiligingsmaatregelen te nemen. Zie voor algemene basismaatregelen de website van het NCSC. [🖱8]*
- *Het NCSC raadt voor weerbaarheid tegen de PetitPotam-aanvalsmethode aan het advies van Microsoft op te volgen: indien mogelijk, schakel NTLM uit.*
- *Veel legacy-systemen blijken afhankelijk te zijn van NTLM waardoor uitschakelen niet altijd triviaal is. In dat geval raadt het NCSC aan het handelingsperspectief van Microsoft op te volgen en het gebruik van NTLM waar mogelijk te beperken. [🖱9] Zie in dit geval ook de NCSC-factsheet 'Zicht op risico's van legacysystemen.' [🖱10]*
- *Installeer beveiligingsupdates ook buiten reguliere patch-rondes zo snel mogelijk; kwetsbaarheden worden binnen een korte tijdsperiode misbruikt.*

Kaseya supplychainaanval zorgt wereldwijd voor ransomware slachtoffers

Op 2 juli vond er een wereldwijde ransomwareaanval plaats waarbij managed serviceproviders (MSP) en hun klanten getroffen werden. Ook in Nederland zijn slachtoffers gevallen. De criminelen achter de ransomware REvil hebben twee kwetsbaarheden in Kaseya VSA misbruikt. Een van de kwetsbaarheden was reeds bekend bij Kaseya dankzij het Dutch Institute for Vulnerability Disclosure (DIVD) die deze kwetsbaarheid en nog 5 andere kwetsbaarheden via een coordinated vulnerability disclosure-traject heeft aangekaart bij Kaseya. De andere misbruikte kwetsbaarheid betrof een nog niet bekende zeroday-kwetsbaarheid. [🖱11] [🖱12] Kaseya VSA is een platform dat het onder andere mogelijk maakt voor MSP's om via een VSA-server systemen van klanten te beheren. Door het compromitteren van een Kaseya VSA-server bij een MSP kunnen systemen van klanten dus ook worden gecompromitteerd. Kaseya heeft op 2 juli alle klanten geadviseerd om de VSA-servers on-premise per direct uit te schakelen. De cloud VSA-servers waren op dat moment al door Kaseya uitgeschakeld. Kaseya heeft klanten met deze producten zelf geïnformeerd. [🖱13] [🖱14] [🖱15] [🖱16]

Op 13 juli verdween REvil van verschillende fora en verdween ook de website die REvil gebruikte om te communiceren met slachtoffers. Kaseya beschikt inmiddels over een decryptor die zij verstrekt hebben aan de getroffen organisaties. De aanvallers eisten een bedrag van 70 miljoen dollar, Kaseya stelt geen bedrag te hebben betaald voor de universele decryptor. [🖱17] [🖱18]

- *In de Maandmonitor van januari, februari en april dit jaar schreef het NCSC reeds over supplychain-aanvallen. Ook het incident bij Kaseya maakt de continue dreiging van supplychain-aanvallen weer duidelijk. Het NCSC adviseert onder andere logging en monitoring in te regelen om supplychain-aanvallen te kunnen detecteren. Hiermee bent u mogelijk ook in staat om vervolgacties van een actor te detecteren.*
- *Zie voor aanvullende informatie over de dreiging van supplychain-aanvallen het rapport van ENISA "Threat Landscape for Supply Chain Attacks". [🖱19]*

Pegasus-spyware toont dreiging mobiele malware

Op 18 juli publiceerde een consortium van 17 nieuwsorganisaties een onderzoek waaruit zou blijken dat dissidenten, mensenrechtenadvocaten, activisten, journalisten en soms ook politici wereldwijd mogelijk doelwit zijn van spionagesoftware Pegasus. [20] [21] Met behulp van deze software, ontwikkeld door de Israëlische NSO Group, kan toegang verkregen worden tot allerlei data van besmette iPhone- en Android-telefoons, zonder dat het slachtoffer zelf enige actie onderneemt: een zogenaamde *zero click*-aanval. Het consortium zegt te beschikken over een lijst van 50.000 telefoonnummers die mogelijk een doelwit vormen. De lijst zelf is niet gepubliceerd. Er zouden ook politici op staan, waaronder de Franse president Emmanuel Macron en voorzitter van de Europese Raad Charles Michel. De NSO Group zou mogelijk nauwe banden onderhouden met Israëlische veiligheidsdiensten. [22] Israël heeft naar aanleiding van de onthullingen een taskforce opgezet om te onderzoeken of er beleidswijzigingen nodig zijn met betrekking tot de export van dergelijke software. [23] [24] De NSO Group zelf stelt de software enkel aan staten te verkopen ten behoeve van criminaliteits- en terrorismebestrijding. [25]

- *In het Cyber Security Beeld Nederland (CSBN) en het Dreigingsbeeld Statelijke Actoren (DBSA) wordt voor het risico van digitale spionage gewaarschuwd. [26] [27]*
- *Het gebruik van spionagesoftware is niet nieuw. Het is dan ook voorstelbaar dat er ook in Nederland slachtoffers zijn van dit soort spionagesoftware.*
- *Besmettingen kunnen worden gedetecteerd door middel van forensisch onderzoek, waarvoor Amnesty International een tool heeft gepubliceerd. [28]*
- *De laagdrempeligheid waarmee geavanceerde aanvalscapaciteiten te verwerven zijn is zorgwekkend, zoals ook aangegeven in het CSBN 2021. [29]*
- *Houd er rekening mee dat gesprekken en berichten ook inzichtelijk kunnen zijn zonder dat de eigen telefoon geïnfecteerd is, bijvoorbeeld wanneer contact verloopt met een telefoon van een gesprekspartner die wel is gecompromitteerd.*
- *In de "Handreiking Cybersecuritymaatregelen" staan acht maatregelen op een rij die elke organisatie zou moeten treffen om cyberaanvallen tegen te gaan. [30]*

Zo sterk als de zwakste schakel

Afgelopen maand hebben de AIVD en de MIVD een publicatie uitgebracht over maatregelen die organisaties kunnen treffen per fase in de Cyber Kill Chain, toegespitst op statelijke actoren. [31] De Cyber Kill Chain is een bekend begrip binnen het cyberdomein. [32] Dit model, bedacht door Lockheed Martin in 2011, [33] beschrijft zeven fasen van activiteiten die kwaadwillenden vaak ondernemen tijdens een aanval. De Cyber Kill Chain wordt door veel organisaties al dan niet in uitgebreidere vorm gebruikt als analysemodel. [34] Hieronder volgt een korte beschrijving van de maatregelen zoals in de publicatie beschreven door de AIVD en MIVD [35], aangevuld met enkele verwijzingen naar NCSC-adviezen. Zie voor meer informatie deze adviezen. [36] [37]

- *Fase 1 – Reconnaissance*
  In deze fase verzamelen aanvallers zoveel mogelijk informatie over zwakke plekken van hun doelwit. Dit kunnen gebouwen, medewerkers, maar ook software en hardware zijn. Preventief maakt u het aanvalsoppervlak zo klein mogelijk. Denk hierbij aan koppelingen met leveranciers of samenwerkingspartners die onderdeel zijn van het aanvalsoppervlak. Zet ongebruikte netwerkpoorten dicht en voorzie uw systemen van de laatste updates. Op het gebied van detectie kunt u actief monitoren op verdachte activiteiten van netwerkverkeer, ook op partnerkoppelingen.
- *Fase 2 – Weaponization*
  Dit is de fase waarin actoren hun 'wapens' kiezen om de aanval mee uit te voeren. Hierbij wordt vaak de afweging gemaakt tussen kosten, capaciteit en slagingskans. Preventief is het van belang om uw kroonjuwelen in kaart te brengen. Daarnaast is het belangrijk bekend te zijn met welke dreiging uitgaat van welke statelijke actor en hoe deze opereert.
- *Fase 3 – Delivery*
  Dit is de aflevering van de payload. Denk hierbij aan een besmette bijlage in een phishingmail. Tegen phishing kunt u diverse maatregelen nemen. Gebruik bijvoorbeeld sandboxes en technieken als DMARC, DKIM en SPF. Zie ook [38]. Het instellen van logging op webpagina's en e-mail is van belang voor detectie en vervolgonderzoek.
- *Fase 4 – Exploitation*
  In deze fase wordt de malware geactiveerd. Hierbij is vaak een actie van een persoon benodigd, bijvoorbeeld het klikken op een malafide link. Het invoeren van 'application whitelisting', het bewustzijn van uw medewerkers vergroten en red teaming-oefeningen zijn maatregelen die u kunt treffen ter preventie.
- *Fase 5 – Installation*
  De toegang is verkregen en wordt uitgebreid. Verhoogde rechten worden ingezet en achterdeurtjes worden geplaatst om die toegang te bestendigen. Om dit tegen te gaan zijn niet alleen segmentering en compartimentering van uw netwerk erg belangrijk, maar ook het instellen van multifactorauthenticatie en beperking van (beheerders)rechten. Zie ook [39].
- *Fase 6 – Command&Control*
  Het besmette systeem communiceert met de Command and Control-server, oftewel C2-verkeer. Hierdoor kan nieuwe malware worden geïnstalleerd. Actieve monitoring op netwerkverkeer kan hierbij helpen om C2-verkeer waar te nemen. Beperk het aantal internetopgangen en gebruik DNS-sinkholing.
- *Fase 7 – Action on Objectives*
  De aanvaller gaat over tot het behalen van het beoogde doel, bijvoorbeeld informatiediefstal of verstoring. Het snel detecteren en beperken van data-exfiltratie is van belang. Evenals het instellen van een incident respons-proces, het oefenen van een crisissituatie en het (laten) veiligstellen van digitale sporen voor forensisch onderzoek.

Overig nieuws Nederland

Overheid wil bedrijven over specifieke cyberdreigingen gaan informeren [40] ■ Kwart ziekenhuizen en GGD's mist basale beveiligingsstandaarden voor websites en e-mail [41] ■ Persoonsgegevens 65.000 ambtenaren op straat door datalek bij ministerie [42] ■ Ontwikkelaar phishingsoftware opgepakt [43] ■ Aanvaller UvA en HvA kwam binnen via besmette laptop van student [44] ■ Toezichthouders publiceren eerste inspectiebeeld cybersecurity vitale processen [45] ■ Vertraging bij Testen voor Toegang blijkt gevolg van hackpoging [46] ■ GGD ging plat door aanvallen op DigiD-leverancier [47] ■ Nederlandse politie neemt servers ransomwaregroep DarkSide in beslag [48] ■ Kamer wil wegens ransomware maatregelen tegen Rusland onderzoeken [49] ■ Kabinet onderzoekt nog of datacenters vitale infrastructuur zijn [50] ■ AIVD wil ruimere wet voor digitale tegenaanvallen [51] ■ Nederland riskeert verlies digitale soevereiniteit [52]