Cyberaanvallen door statelijke actoren:

zeven momenten om een aanval te stoppen

Cyberaanvallen door statelijke actoren:

zeven momenten om een aanval te stoppen

Hoe wordt u aangevallen en wat kunt u ertegen doen?

De Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en de Militaire Inlichtingen- en Veiligheidsdienst (MIVD) zien dat Nederlandse (overheids-) organisaties en bedrijven op grote schaal digitaal worden aangevallen door statelijke actoren.* Mede doordat steeds meer staten digitale aanvallen uitvoeren, is de cyberdreiging tegen Nederland de afgelopen jaren sterk toegenomen. Deze aanvallen raken onze economie, onze welvaart en onze veiligheid.

* Op de AIVD-website vindt u de eerdere publicatie “Offensief cyberprogramma: een ideaal businessmodel voor staten” uit 2019. Hierin leest u meer over de aantrekkelijkheid van een offensief cyberprogramma voor statelijke actoren.

Deze publicatie waarschuwt bestuurders, beleidsmakers en managers voor de werkwijze van statelijke actoren en geeft advies voor het verhogen van de digitale weerbaarheid tegen statelijke cyberaanvallen. Neem deze brochure mee als u in gesprek gaat met ICT-beveiligers over de digitale weerbaarheid van uw organisatie. Een goede samenwerking tussen bestuurders, beleidsmakers, managers en ICT-beveiligers is bepalend voor de effectiviteit en het succes van de gekozen beveiligingsstrategie.

U kunt de kans op succesvolle cyberaanvallen verkleinen door de werkwijze van statelijke actoren te begrijpen. Om u inzicht te geven in de werkwijze van cyberaanvallen en wat u hiertegen kunt doen, nemen we u mee in de verschillende fasen van een cyberaanval. Hiervoor zijn verschillende modellen te gebruiken. In deze brochure hebben we gekozen voor het model van de Cyber Kill Chain.

De Cyber Kill Chain
De Cyber Kill Chain is een hulpmiddel dat wereldwijd gebruikt wordt om inzicht te geven in de werkwijze van cyberaanvallers. Dit model beschrijft de zeven fasen die aanvallers kunnen doorlopen om hun doel te bereiken. In de praktijk worden niet altijd alle fasen van een cyberaanval doorlopen of worden bepaalde fasen, om steeds dieper een netwerk binnen te dringen, juist meerdere keren doorlopen.

Deze publicatie legt de theorie van de Cyber Kill Chain uit en gebruikt hierbij de vergelijking met een fysieke inbraak in een villa. Per fase wordt ook een praktijkvoorbeeld van een statelijke cyberaanval toegelicht. Tot slot geeft iedere fase advies over maatregelen om aanvallers te ontdekken, vertragen of stoppen. Het tijdig kunnen ontdekken en stoppen van aanvallers zorgt ervoor dat zij opnieuw hun aanval moeten beginnen. Als aanvallers keer op keer hiertoe gedwongen worden, moeten zij een grotere inspanning leveren waardoor de kosten van een aanval flink toenemen. De kans dat aanvallers hun aanvalspoging herhalen wordt hierdoor kleiner.

De beveiligingsmaatregelen zijn onderverdeeld in preventieve en detectieve maatregelen. Het is niet mogelijk om per fase een volledige weergave van alle beveiligingsmaatregelen te geven. Daarom is het belangrijk dat u de werkwijze van aanvallers begrijpt en met ICT-beveiligers onderzoekt welke beveiligingsmaatregelen passen bij uw organisatie en beveiligingsstrategie. U kunt hierbij het advies per fase als uitgangspunt gebruiken. Zo kunt u zorgen voor een hogere digitale weerbaarheid van uw organisatie. Wanneer uw organisatie geen security-afdeling heeft, kunt u voor het implementeren van beveiligingsmaatregelen gebruikmaken van een externe partner voor security-dienstverlening.


101010
01010
1010
RECONNAISSANCE
WEAPONIZATION
DELIVERY
EXPLOITATION
INSTALLATION
COMMAND AND CONTROL
ACTIONS ON OBJECTIVES

Fase 1:
Reconnaissance

In de eerste fase selecteren aanvallers hun doelwitten. Daarna worden digitale verkenningen uitgevoerd om zoveel mogelijk informatie over de zwakke plekken van deze doelwitten te verzamelen. Zwakke plekken kunnen zowel personen als technische kwetsbaarheden zijn.

Vergelijking met een fysieke inbraak

Inbrekers die op zoek zijn naar meesterwerken van beroemde kunstschilders kiezen andere doelwitten uit dan inbrekers die geïnteresseerd zijn in juwelen. Als de doelwitten eenmaal gekozen zijn, gaan ze de omgeving van de doelwitten fysiek verkennen. Ze verkennen de wegen die naar hun doelwitten leiden. Ook onderzoeken ze op welk tijdstip bepaalde mensen aanwezig zijn, of er alarmsystemen zijn en of er camera's hangen. Daarnaast gaan ze op zoek naar deuren die niet op slot zitten of ramen die vaak openstaan. Ook zoeken inbrekers uit of er mensen werken die ze kunnen helpen om binnen te komen, bijvoorbeeld een glazenwasser waarvan ze de ladder kunnen gebruiken.

In de Reconnaissance-fase verzamelen cyberaanvallers zoveel mogelijk informatie over de zwakke plekken van hun doelwit. Deze informatie hebben zij nodig om in de volgende fasen van de Cyber Kill Chain toegang te krijgen. In het voorbeeld hierboven gaan de inbrekers gericht te werk. In de praktijk kiezen cyberaanvallers ook doelwitten opportuun uit op basis van een zwakke plek die misbruikt kan worden. Denk hierbij aan een publicatie over een kritieke kwetsbaarheid in software. Statelijke cyberaanvallers gaan na deze publicatie op zoek naar doelwitten die gebruikmaken van deze software in plaats van eerst hun doelwitten te selecteren.

Advies – wat kunt u doen?

In de Reconnaissance-fase verzamelen cyberaanvallers zoveel mogelijk informatie om het aanvalsoppervlak in kaart te brengen. Het is daarom belangrijk om beveiligingsmaatregelen te kiezen die gericht bijdragen aan het verkleinen van het aanvalsoppervlak van uw organisatie.

Preventieve beveiligingsmaatregelen

- Sommige statelijke cyberaanvallers scannen automatisch op bekende kwetsbaarheden in systemen en apparaten die gekoppeld zijn met het internet. Ook scannen actoren op openstaande poorten om inzicht in de infrastructuur van uw organisatie te krijgen. Poorten zijn de toegangen waarop informatie wordt ontvangen en verstuurd via het internet. Bij veel bedrijven en organisaties staan standaard te veel poorten open, ook als ze niet gebruikt worden. Zet ongebruikte poorten daarom dicht, houd aan het internet gekoppelde systemen en apparaten up-to-date en voorzie ze van de laatste patches en configuraties. Houd uw Configuration Management Database (CMDB) bij zodat u snel kunt reageren op updates en securitypatches van leveranciers.

- Koppelingen met het netwerk van een leverancier of samenwerkingspartner zijn ook onderdeel van het aanvalsoppervlak. Als het netwerk van uw leverancier of samenwerkingspartner onvoldoende beveiligd is, kan dit de zwakke plek van uw organisatie zijn. Aanvallen op bedrijven of organisaties via een toeleverancier of samenwerkingspartner, worden supply chain-aanvallen genoemd. Deze aanvallen behoren tot de standaard werkwijze van verschillende statelijke cyberaanvallers. Om het risico op supply chain-aanvallen te verkleinen, is het belangrijk dat u partnerkoppelingen niet standaard als vertrouwd beschouwd en eisen stelt aan de beveiliging van de systemen van uw partners.

- In de Reconnaissance-fase zoeken aanvallers ook op internet naar openbare informatie over uw organisatie of medewerkers. Zo zoeken ze op internet bijvoorbeeld naar gebruikte technieken, systemen, software of hardware van een organisatie, of naar e-mailadressen van medewerkers. Aanvallers gebruiken dit soort informatie om kwetsbaarheden te vinden, maar ook om een geloofwaardige (spear)phishingmail op te stellen. Het bewustzijn en handelen van uw medewerkers speelt daarom een belangrijke rol bij het verkleinen van het aanvalsoppervlak. Maak medewerkers bewust van de risico's van het delen van persoonlijke informatie, functieomschrijvingen en informatie over gebruikte ICT-componenten en configuraties op sociale media, zoals Facebook of LinkedIn.

Detectieve beveiligingsmaatregelen

- In deze fase kunt u verkenningen ontdekken door gebruik te maken van detectieoplossingen. Denk hierbij aan het gebruik van een zogeheten Network based Intrusion Detection System (NIDS). Zo kunt u het inkomend en uitgaand netwerkverkeer, ook op partnerkoppelingen, actief monitoren en analyseren op verdachte activiteiten.

Close-access hackoperatie op OPCW

Op 13 april 2018 staat een auto geparkeerd bij het Marriott hotel in Den Haag. Op de hoedenplank van de auto ligt, verstopt onder een jas, een antenne. Deze antenne staat gericht op het hoofdkwartier van de Organisation for the Prohibition of Chemical Weapons (OPCW) en is gekoppeld aan apparatuur waarmee op afstand het verkeer van wifi-netwerken kan worden onderschept. Hiermee kunnen gebruikers van het wifi-netwerk herkend worden en hun inloggegevens achterhaald. De apparatuur in de achterbak van de auto is zowel met een gekoppelde laptop als op afstand aan te sturen via een 4G-verbinding. Het is duidelijk: de verkenningsfase van een cyberaanval is begonnen.

De auto is gehuurd door vier inlichtingenofficieren van een zogenoemd close-access hacking team van de Russische militaire inlichtingendienst GRU. Close-access teams proberen fysiek zo dicht mogelijk bij hun doelwit te komen, zodat ze toegang kunnen krijgen tot netwerken die niet direct via het internet te benaderen zijn, zoals interne wifi-netwerken. In de Reconnaissance-fase worden deze netwerken op locatie herkend.

Door een contra-inlichtingenoperatie kon de MIVD op 13 april de close-access hack-operatie van de GRU op de OPCW al in de Reconnaissance-fase herkennen en verstoren.

Fase 2:
Weaponization

Als aanvallers een zwakke plek hebben gevonden ontwikkelen ze gereedschap, bijvoorbeeld malware, om deze te misbruiken.

Vergelijking met een fysieke inbraak

De inbrekers hebben besloten om in te breken in de villa van het doelwit. Tijdens hun verkenningen zijn zij erachter gekomen dat een raam standaard openstaat. Een simpel haakje voorkomt dat het raam openwaait. In de Weaponization-fase verbuigen de inbrekers thuis een kleerhanger, die zij door de kier van het raam kunnen steken om het haakje omhoog te wippen.

Cyberaanvallen werken op dezelfde manier als in het voorbeeld hierboven. Ook statelijke actoren kiezen op basis van hun verkenningen welke kwetsbaarheid ze willen misbruiken. Tijdens de Weaponization-fase kiezen of ontwikkelen actoren gereedschap met een zo hoog mogelijke slagingskans.

Statelijke actoren maken vaak gebruik van bekende kwetsbaarheden in software waarvoor al exploits (software die kwetsbaarheden misbruiken) bestaan. Aanvallers zetten exploits in om toegang te krijgen tot systemen. Via deze toegang kan vervolgens malware (kwaadaardige software) worden geïnstalleerd, waarmee de aanvallers controle kunnen krijgen over deze systemen.

Statelijke actoren kunnen ook gebruikmaken van kwetsbaarheden die nog niet publiekelijk bekend zijn. Deze hebben aanvallers ontdekt of voor veel geld gekocht op een online zwarte markt. Dit type kwetsbaarheden worden zero-days genoemd.

Advies – wat kunt u doen?

In de Weaponization-fase bereiden aanvallers zich voor op een cyberaanval. In deze fase is er nog geen interactie met het doelwit. Daarom is het zeer lastig om de aanvaller in deze fase te herkennen of stoppen. Dit betekent niet dat u niets kunt doen.

- Breng uw kroonjuwelen in kaart en onderzoek voor welke statelijke actoren u een voorstelbaar doelwit vormt. In verschillende publicaties op de website van de AIVD kunt u hier meer over lezen.

- Als u weet voor welke statelijke actoren u een voorstelbaar doelwit vormt, kunt u onderzoeken welke aanvalstechnieken deze actoren gebruiken. Een veelgebruikt raamwerk dat een grote diversiteit aan aanvalstechnieken per statelijke actor in kaart heeft gebracht, is het MITRE ATT&CK Framework.* Onderzoek met dit model of u beveiligingsmaatregelen heeft genomen tegen bekende aanvalstechnieken voor uw organisatie. Tot slot kunt u nagaan of de detectiemaatregelen van uw organisatie deze aanvalstechnieken kunnen ontdekken.

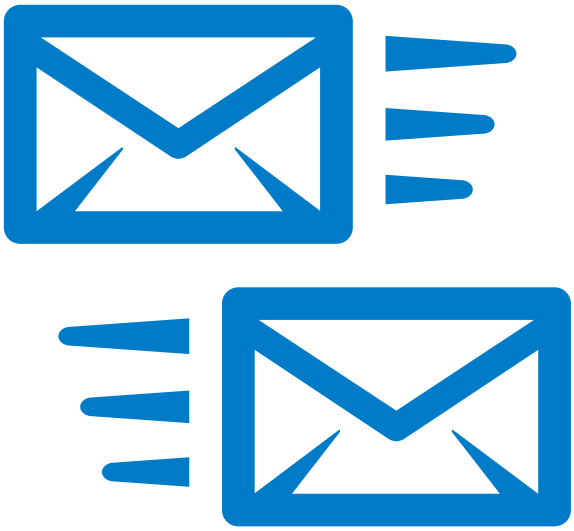
* https://attack.mitre.org

Waarschuwing vanuit AIVD, MIVD en NCSC zorgt voor 'Citrix-files'

In de ochtend van maandag 20 januari 2020 luidt de verkeersinformatie als volgt: "Het verkeer dient rekening te houden met een drukkere spits vanwege kans op gladheid, dichte mist en problemen met Citrix-servers". Die laatste vertragingsoorzaak is zeer ongebruikelijk. De vrijdag daarvoor zijn op aanraden van de AIVD, MIVD en het Nationaal Cyber Security Centrum (NCSC) servers bij de overheid en diverse bedrijven offline gehaald waarop Citrix-software draaide. Met deze software kunnen medewerkers vanuit huis op afstand inloggen op het bedrijfsnetwerk van hun overheidsinstantie of bedrijf.

De AIVD en MIVD zien in de dagen voor de uitgebrachte waarschuwing dat een statelijke actor een bekende kwetsbaarheid in Citrix-VPN-servers actief probeert in te zetten voor cyberspionagedoelen.

De kwetsbaarheid in de Citrix-servers is begin december 2019 openbaar gemaakt op internet. Vervolgens is op 10 januari 2020 via diverse internetfora gepubliceerd hoe de kwetsbaarheid daadwerkelijk misbruikt kan worden om binnen te dringen in interne netwerken. Deze informatie wordt door statelijke actoren razendsnel gebruikt om systemen te identificeren waarop de bewuste kwetsbaarheid in de Citrix-software nog aanwezig is. Vervolgens lukte het statelijke actoren om in de Weaponization-fase binnen enkele dagen een exploit te ontwikkelen, waarmee ze actief misbruik konden maken van de Citrix-kwetsbaarheid.



Fase 3:
Delivery

Als het doelwit geselecteerd is en de malware klaar ligt voor gebruik, bezorgen de aanvallers de malware bij de organisatie met behulp van bijvoorbeeld een e-mail.

Vergelijking met een fysieke inbraak

De inbrekers rijden met de omgebogen kleerhanger achterin hun bus naar de villa.

Het afleveren van het gereedschap om mee in te breken werkt in de digitale wereld anders dan in de fysieke wereld, omdat de dimensies 'tijd' en 'afstand' een minder grote rol spelen. In de fysieke wereld kost het inbrekers bijvoorbeeld een half uur om naar hun doelwit te rijden. Bij een cyberaanval vervalt deze dimensie, omdat bijvoorbeeld een (spear) phishingmail in een oogwenk verstuurd en afgeleverd kan worden.

Het versturen van (spear)phishingmails is daarom een veelgebruikte methode om malware bij het slachtoffer af te leveren. Aanvallers maken bijvoorbeeld e-mails die aansluiten op een actueel onderwerp met daarin een link naar een bijpassend artikel of een bijlage met een interessante titel. Hoewel de lezer daadwerkelijk een artikel te lezen krijgt als hij op de link of bijlage klikt, opent op de achtergrond ook malware die zich in het systeem van het slachtoffer nestelt. Een aanval met een (spear)phishingmail werkt op dezelfde manier, maar is geraffineerder omdat die e-mail op een specifiek slachtoffer is toegespitst. Aanvallers gebruiken hiervoor vaak de informatie die ze in de verkenningsfase hebben gevonden.

Een andere veelgebruikte methode die aanvallers gebruiken om hun malware op het systeem van hun beoogde doelwit af te leveren, is het hacken van een website die kwetsbaarheden bevat en die vaak bezocht wordt door medewerkers. Op deze website brengen de aanvallers vervolgens malware aan waardoor bezoekers geïnfecteerd worden zodra ze de website bezoeken. Zo'n aanval wordt een watering hole attack genoemd. Ook kunnen aanvallers gratis USB-sticks uitdelen waarop al malware geïnstalleerd staat, in de hoop dat medewerkers van het beoogde doelwit de USB-sticks gebruiken op de systemen van de organisatie.

Advies – wat kunt u doen?

In de Delivery-fase moeten beveiligingsmaatregelen gekozen worden die voorkomen dat de malware die in de Weaponization-fase is ontwikkeld, daadwerkelijk wordt afgeleverd.

Preventieve beveiligingsmaatregelen

- In deze fase is het belangrijk om inkomende e-mails en eventuele bijlagen te scannen op malware en verdachte URL's. Zo kunt u e-mails op een mailproxy scannen om ervoor te zorgen dat eventuele malware geblokkeerd wordt en nooit de inbox van de gebruiker bereikt. U kunt ook gebruikmaken van sandboxes (een geïsoleerde omgeving die niet gekoppeld is met het bedrijfsnetwerk) op de mailserver die controles uitvoeren en eventuele malware blokkeren.

- Controleer daarnaast de herkomst van e-mails aan de hand van technieken als Domain-based Message Authentication, Reporting and Conformance (DMARC), Domain Keys Identified Mail (DKIM) of Sender Policy Framework (SPF). Deze technieken blokkeren e-mails van onbekende herkomst. Ook kunt u met behulp van policies instellen dat

uitvoerbare bestandstypen als .exe of .msi niet zijn toegestaan in de bijlage van een e-mail, zodat deze niet in de inbox van een gebruiker kunnen komen. Als er verdachte kenmerken in een e-mail of bijlage gevonden worden, is het belangrijk om de e-mail in quarantaine te plaatsen voor verder onderzoek en deze niet te verwijderen. Als u de e-mail verwijdert, kan er geen onderzoek meer gedaan worden.

- Daarnaast kunt u browsers en applicaties hardenen om het risico te verkleinen dat systemen van medewerkers besmet kunnen raken door het bezoeken van geïnfecteerde webpagina's. Met het hardenen van browsers wordt bijvoorbeeld het uitschakelen van plug-ins bedoeld die als kwetsbaar bekend staan. Denk bij het hardenen van applicaties aan het uitschakelen van Office macro's die de gebruiker niet nodig heeft. Macro's worden vaak ingezet om malware over te brengen.

- Stel ook beleid op voor het gebruik van verwijderbare media en datadragers en het koppelen van eigen hardware (Bring Your Own Device) met het bedrijfsnetwerk. Denk hierbij bijvoorbeeld aan USB-sticks. Zet USB-poorten dicht en sta alleen geregistreerde USB-media toe die is uitgegeven en onder controle is van de eigen organisatie. Schakel daarbij ook de autorun-functionaliteit uit op verschillende media.

Detectieve beveiligingsmaatregelen

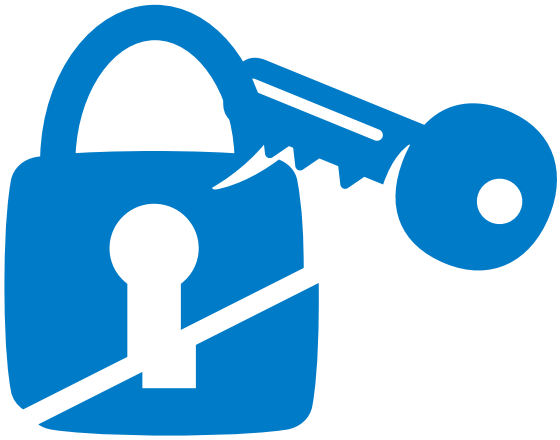
- Door webpagina's te loggen die gebruikers bezoeken, kunt u analyseren of er geïnfecteerde webpagina's bezocht zijn. Hiervoor zijn verschillende beveiligingsproducten beschikbaar. Logging van e-mail en webpagina's is nodig om onderzoek te kunnen doen zodra u een aanvaller ontdekt. Als u niet over deze logging beschikt is het lastig vast te stellen wanneer en hoe de malware bezorgd is.

- Het gebruik van een antivirusprogramma of een Next-Generation Antivirus (NGAV) helpt in de Delivery-fase bij het vinden van eventuele malware.

Cyberaanvallen op Nederlandse ministeries

Het is eind 2018 als phishingmails opduiken in de mailboxen van diverse medewerkers van een Nederlands ministerie. Een statelijke actor probeert met betrouwbaar ogende inhoud en specifiek gekozen bewoordingen medewerkers te verleiden om de bijlage met malware te openen. Het filtersysteem van de e-mailserver doet zijn werk en ontdekt en verwijdert de malware uit de phishingmails. In dit geval is bezorging van de phishingmails in de Delivery-fase voorkomen.

De AIVD en MIVD zien regelmatig digitale spionagepogingen van statelijke actoren bij meerdere Nederlandse ministeries. Er is één ministerie dat de laatste jaren op extra aandacht van statelijke actoren lijkt te kunnen rekenen: het ministerie van Buitenlandse Zaken. Zo heeft de AIVD gezien dat een aantal Nederlandse ambassades in het Midden-Oosten en Centraal-Azië tussen 2017 en 2020 doelwit is geweest van digitale aanvallen, uitgevoerd door een buitenlandse inlichtingendienst. Doel was waarschijnlijk inzicht te krijgen in het e-mailverkeer tussen een Nederlandse diplomatieke post in het buitenland en het ministerie van Buitenlandse Zaken in Nederland.



Fase 4:
Exploitation

In deze fase wordt de malware geactiveerd, doordat bijvoorbeeld een van de medewerkers op een link in een malafide e-mail klikt.

Vergelijking met een fysieke inbraak

Een van de inbrekers steekt zijn omgebogen kleerhanger door de kier van het raam en wipt het haakje waarmee het raam vastzit open. In deze fase klimt de inbreker nog niet naar binnen. Hij heeft alleen toegang voor zichzelf weten te creëren.

Het laatste deel om toegang te krijgen gebeurt in de Exploitation-fase. Aanvallers moeten het 'raam' nog forceren. De Exploitation-fase is daarom gericht op het activeren van de malware. Denk hierbij aan een medewerker die op de link in de (spear)phishingmail moet klikken om de malware te activeren waarmee aanvallers toegang kunnen krijgen.

Geavanceerde cyberaanvallers, zoals statelijke actoren, zetten alles op alles om de kans te vergroten dat een medewerker op een link klikt of een malafide bijlage opent. De kans dat dit lukt is groter als een e-mail betrouwbaar oogt. Aanvallers kunnen dit bijvoorbeeld doen door toegang te krijgen tot het e-mailaccount van de directeur van een bedrijf en e-mails namens deze persoon te versturen. Aanvallers kunnen ook e-mails versturen vanuit hun eigen infrastructuur en zich voordoen als iemand anders. De ontvanger denkt dan dat de phishingmail afkomstig is van een betrouwbare partij. Dit wordt spoofing genoemd.

Advies – wat kunt u doen?

Aanvallers hebben in deze fase nog geen stevige voet aan de grond. De beveiligingsmaatregelen in deze fase richten zich op het ontdekken en blokkeren van kwaadaardige code of scripts.

Preventieve beveiligingsmaatregelen

- Maak in deze fase gebruik van application whitelisting. Deze maatregel verbiedt alle software op systemen met uitzondering van software die op een door de organisatie samengestelde vertrouwde lijst (whitelist) staat. Hiermee verlaagt u het risico dat malware kan worden geïnstalleerd of uitgevoerd.

- Aanvallers proberen gebruikers in deze fase te misleiden om een handeling uit te voeren. Maak uw medewerkers daarom bewust van de risico's van (spear)phishing en het klikken op onbekende links. Adviseer medewerkers om eerst de afzender van een verdachte e-mail te bellen of te mailen voor zij de bijlage of URL openen.

Detectieve beveiligingsmaatregelen

- Door een Endpoint Detection and Response (EDR)-oplossing te gebruiken, kunt u kwaadaardige code of scripts in de vorm van virussen, malware, ransomware of andere verdachte activiteiten tijdig ontdekken en blokkeren. Deze oplossingen kunnen worden ingezet op zowel desktops, laptops, smartphones als servers.

- Het is belangrijk om periodieke beveiligingstesten als kwetsbaarhedenscans, pentesten en red teaming-oefeningen uit te voeren, zodat u kwetsbaarheden en gevonden toegangspaden tijdig kunt mitigeren. Een ICT-infrastructuur is namelijk continu aan

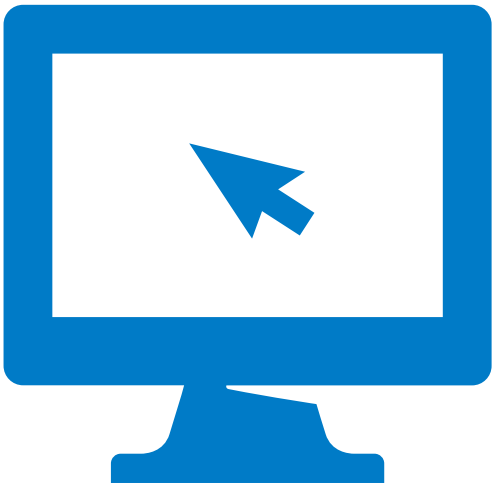
verandering onderhevig waardoor kwetsbaarheden kunnen ontstaan; nieuwe systemen worden aangesloten, oude systemen worden geüpdatet en configuraties van netwerk-apparatuur worden regelmatig aangepast.

Statelijke actoren maken digitaal misbruik van COVID-19-pandemie

Bij de AIVD en MIVD komen al snel na het uitbreken van de COVID-19-pandemie signalen binnen dat sommige statelijke actoren in het geheim toch wat minder op hebben met de wereldwijde gezamenlijke zoektocht naar een vaccin in de strijd tegen het coronavirus. Ze blijken hun eigen voordeel te willen doen met onderzoeksresultaten van farmaceutische bedrijven uit andere landen.

Bij diverse bedrijven en onderzoeksinstellingen die betrokken zijn bij de preventie en bestrijding van het coronavirus komen e-mails binnen die op het eerste oog te maken hebben met de gezamenlijke strijd tegen het virus. Maar als iemand de e-mail en de bijlage met informatie opent, gaat het mis: de malware van de statelijke actor is geactiveerd en kan zich installeren op het netwerk.

Het blijkt te gaan om phishingmails van statelijke actoren. Door de ernst van de pandemie zijn diverse ontvangers van deze e-mails minder op hun hoede bij de beoordeling van de afzender en inhoud van de e-mail, en openen de linkjes of bijlagen met malware. Hiermee is de Exploitation-fase geslaagd en zijn statelijke actoren digitaal binnengedrongen bij diverse bedrijven en onderzoeksinstellingen wereldwijd.



Fase 5:
Installation

In de installatiefase nestelen aanvallers zich in het netwerk van het doelwit en proberen hierbij permanente toegang te krijgen.

Vergelijking met een fysieke inbraak

De inbreker klimt in deze fase door het raam de villa binnen en zet zijn telefoon aan, zodat hij in de volgende fase contact kan opnemen met zijn handlanger. Vervolgens gaat hij de villa zo geruisloos mogelijk verkennen: op kousenvoeten en zonder lampen aan te doen. Hierbij kan hij op deuren stuiten die gesloten zijn of een kluis tegenkomen. Afhankelijk van de gereedschappen die hij zelf heeft meegenomen, kan hij deze openen. Anders moet hij hiermee wachten tot hij (in de volgende fase) contact heeft gehad met zijn handlanger.

Als statelijke aanvallers toegang tot het computersysteem van het doelwit hebben gekregen, proberen ze zo snel mogelijk de meest uitgebreide rechten binnen het netwerk te krijgen. Dit zijn bij voorkeur de rechten van een beheerder. Met deze rechten is het mogelijk om het netwerk zo uitgebreid mogelijk te verkennen. Dit wordt lateraal bewegen genoemd.

Statelijke actoren gaan daarbij vaak zeer geavanceerd te werk. Zij kunnen zich vrijwel onzichtbaar door een systeem bewegen. Eén van de redenen voor lateraal bewegen is om permanente toegang te krijgen door bijvoorbeeld zogenoemde 'achterdeuren' te plaatsen. De uitgebreide rechten maken het voor de aanvaller ook mogelijk om binnen het hele netwerk op zoek te gaan naar de plekken waar de meest interessante data staat.

Door het geduld en het doorzettingsvermogen van statelijke actoren om toegang te krijgen tot computersystemen, de tijd die ze in deze installatiefase nemen om de gewenste informatie ongezien buit te kunnen maken en de geavanceerde technieken die ze hiervoor inzetten, worden statelijke cyberactoren in de cybersecuritywereld Advanced Persistent Threats (APT's) genoemd.

Advies – wat kunt u doen?

Kies in deze fase beveiligingsmaatregelen die voorkomen dat aanvallers zich permanent op meerdere plekken in het netwerk kunnen nestelen.

Preventieve beveiligingsmaatregelen

- Als de malware succesvol geïnstalleerd is, wilt u voorkomen dat aanvallers zich lateraal kunnen bewegen. Een effectieve maatregel hiervoor is het compartimenteren van systemen en het segmenteren van netwerken. Compartimenteren doet u door niet noodzakelijke verbindingen uit te schakelen. Bij segmenteren deelt u het netwerk in verschillende stukken in. Zo beperkt u de toegang tot vertrouwelijke informatie of kritieke processen tot de medewerkers, applicaties en computers die deze toegang daadwerkelijk nodig hebben. Segmenteren kan redelijk eenvoudig gerealiseerd worden met Virtual Local Area Networks (VLAN's) en firewalls.

- Ook is het minimaliseren van rechten belangrijk. Beperk daarom het aantal beheerders-accounts en beperk de rechten voor beheerdersactiviteiten binnen deze accounts. Scherm daarnaast de identiteit van deze accounts af. Geef ook niet meer rechten aan accounts

van reguliere gebruikers dan noodzakelijk is (principle of least privilege). Gehackte accounts kunnen hierdoor beperkt gebruikt worden voor verdere verkenningen van het systeem of netwerk. Schakel een beheerdersaccount uit, zodra deze niet meer gebruikt wordt. Gebruik tot slot verschillende accounts en sterke wachtwoorden voor beheerderstaken, en bepaal welke beheerdersactiviteiten op afstand uitgevoerd mogen worden. Blokkeer daarnaast standaard protocollen zoals RDP (Remote Desktop Protocol) of Telnet, of plaats deze achter een VPN.

- Multifactorauthenticatie (MFA) is niet alleen een belangrijke beveiligingsmaatregel waarmee u voorkomt dat aanvallers toegang krijgen, het verhindert in deze fase ook dat aanvallers lateraal kunnen bewegen met eventueel buitgemaakte credentials. Bij multifactorauthenticatie moet aan een combinatie van meerdere factoren voldaan worden om toegang te krijgen tot een functionaliteit of applicatie. Bijvoorbeeld het gebruik van een vingerafdruk of smartcard in combinatie met een wachtwoord. Stel multifactorauthenticatie ook verplicht bij het gebruik van een VPN. Aanvallers krijgen hierdoor geen externe toegang tot het bedrijfsnetwerk als zij de credentials van een gebruiker hebben verkregen.

Detectieve beveiligingsmaatregelen

- Als u een Security Operations Center (SOC) heeft, kunt u samen een detectiestrategie bepalen. Een SOC maakt gebruik van een Security Information & Event Management-systeem (SIEM) waar logging en relevante data centraal op binnenkomen. Zij kunnen bijvoorbeeld zien of accounts hebben ingelogd die eerder nog niet actief waren of waarbij de laatste inlogpoging langere tijd geleden was. Als er meerdere foutieve inlogpogingen zijn gezien is dit verdacht.

- Een SOC kan daarbij ook vaststellen of gebruikersaccounts extra rechten hebben gekregen of onderdeel zijn geworden van de beheerdersgroep en onderzoeken of deze wijziging klopt. Als u geen SOC heeft, kunt u overwegen om een security dienstverlener in te schakelen.

Langdurige hack EU-ambassade Moskou

Op 5 juni 2019 bericht nieuwsplatform Buzzfeed over een “geavanceerd cyberspionage incident”. Naar verluidt zou een Russische APT van februari 2017 tot en met april 2019 toegang hebben gehad tot digitale systemen van de EU-ambassade in Moskou. Een interne analyse, ingezien door Buzzfeed, laat zien dat minstens twee computers geïnfecteerd zijn met malware van de APT en dat informatie is gestolen. De aard en omvang van de buitgemaakte informatie is onduidelijk. EU-woordvoering staat voorafgaand aan de publicatie met journalisten in contact en bevestigt desgevraagd dat het incident heeft plaatsgevonden en dat vervolgonderzoek gaande was.

Dergelijke cyberspionage door statelijke actoren toont aan dat APT’s de middelen en mogelijkheden hebben om zich ongezien toegang te verschaffen tot gevoelige digitale systemen. Als ze in de Installation-fase de Cyber Kill Chain zorgvuldig doorlopen, kunnen ze ook voor een langere tijd ongezien op een netwerk actief blijven.

Fase 6:
Command and Control

In deze fase leggen de aanvallers op afstand contact met de geïnstalleerde malware binnen het netwerk en kunnen via dit communicatiekanaal nieuwe malware installeren.

Vergelijking met een fysieke inbraak

De fysieke inbreker neemt contact op met zijn handlanger. Die geeft hem instructies en voorziet hem van extra gereedschappen die hij nodig heeft. Soms bestaat dat gereedschap uit een (inlog)code voor een computer of een kluis die telefonisch doorgegeven kan worden. Vaak zal de inbreker een achterdeur van het slot doen om gereedschappen aangereikt te krijgen. Hiermee creëert de inbreker ook meteen een andere in- en uitgang voor zichzelf als het raam geen optie meer is als uitgang.

In de digitale wereld neemt de malware op enig moment na de installatie contact op met de Command and Control-server, ook wel C2-server genoemd. De aanvaller heeft in deze fase permanente toegang tot het netwerk gekregen en kan op afstand de malware via de achterdeuren die hij in de Installation-fase heeft geplaatst besturen en nieuwe malware het netwerk binnenbrengen.

Deze communicatie wordt Command and Control-verkeer (C2-verkeer) genoemd.
Met nieuwe malware kunnen aanvallers nog dieper het netwerk binnendringen om op zoek te gaan naar de data waarin zij geïnteresseerd zijn.

Advies – wat kunt u doen?

Deze fase is het laatste moment dat u heeft om ervoor te zorgen dat aanvallers niet de volgende en laatste stap kunnen zetten. In deze fase moeten beveiligingsmaatregelen gekozen worden die het C2-verkeer ontdekken en voorkomen dat aanvallers via de C2-server kunnen communiceren.

Preventieve beveiligingsmaatregelen

- In deze fase wilt u de kans verkleinen dat aanvallers succesvol hun C2-server kunnen aanspreken. Beperk bijvoorbeeld het aantal internetopgangen, zodat aanvallers minder geschikte plekken hebben om achterdeuren te plaatsen. Ook kan al het netwerkverkeer via een proxy of next-generation firewall (NGFW) geleid worden. Een proxy kan op afwijkend verkeer filteren waardoor C2-verkeer geblokkeerd wordt.

- Daarnaast kunt u gebruikmaken van DNS-sinkholing. Dit is een techniek waarbij domeinnamen die aanvallers voor hun C2-server gebruiken niet meer geresolved worden. In de praktijk zorgt deze beveiligingsmaatregel ervoor dat er geen verkeer meer mogelijk is tussen het organisatienetwerk en de C2-server van aanvallers.

Detectieve beveiligingsmaatregelen

- In deze fase wordt contact gemaakt met de C2-server van de aanvallers. Dit C2-verkeer kunt u waarnemen. De communicatie tussen de malware en aanvallers kan verstopt worden in regulier netwerkverkeer, bijvoorbeeld in de communicatie tussen uw netwerk en een nieuwswebsite die uw medewerkers regelmatig bezoeken. Ook is het mogelijk dat de communicatie via een clouddienst verloopt. Als aanvallers gebruikmaken van deze technieken, kunnen ze lastiger ontdekt worden.

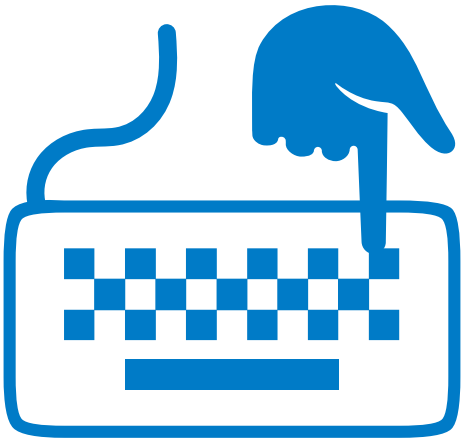
- Om deze communicatie toch op te merken, moet u zorgen voor actieve monitoring. U let daarbij bijvoorbeeld op verdachte hoeveelheden netwerkverkeer en ongebruikelijke datastromen. Om vast te stellen wat verdacht netwerkverkeer is, kunt u ook gebruikmaken van indicatoren in openbare of commerciële rapporten over cyberaanvallen die wijzen op C2-infrastructuren.

Nederlandse ICT-infrastructuur gebruikt door statelijke actoren bij cyberoperaties

De afgelopen jaren ontving de AIVD veel berichten van inlichtingen- en veiligheidsdiensten van andere Europese landen dat bedrijven en overheden in hun land aangevallen werden vanuit Nederland. Voerden Nederlandse hackers aanvallen uit op die doelen of was de werkelijkheid ingewikkelder?

Dat cyberaanvallen via Nederlandse ICT-infrastructuur verlopen is niet vreemd, omdat veel internetverkeer via Nederland loopt. In Amsterdam en in de Eemshaven in Groningen zitten twee van de belangrijkste internetknooppunten in de wereld. Het internetknooppunt in Amsterdam is zelfs het grootste van Europa. Daarnaast is het, ook voor statelijke actoren, aantrekkelijk om servers te huren in Nederland. Nederland is een van de best bekabelde landen in de wereld, waardoor internetverbindingen snel en betrouwbaar zijn. Hierdoor is ons land ook populair voor datacenters, waardoor servers relatief goedkoop gehuurd kunnen worden. Ook buitenlandse aanbieders van servers huren deze geregeld in Nederland. Daardoor verlopen aanvallen vanuit servers die ingehuurd zijn bij zo'n buitenlandse partij alsnog via Nederlandse infrastructuur.

De AIVD en MIVD hebben de afgelopen jaren in toenemende mate gezien dat statelijke actoren gebruikmaken van deze Nederlandse servers bij cyberaanvallen. Deze servers worden door statelijke actoren vaak gebruikt als Command and Control-server voor hun cyberoperaties. Hierdoor wordt Nederland onderdeel van cyberoperaties waar het niets mee te maken heeft.



Fase 7:
Actions on Objectives

Vanaf het moment dat aanvallers permanente toegang hebben gekregen, kunnen zij zich focussen op het bereiken van het doel waarvoor ze de cyberaanval zijn gestart, bijvoorbeeld het ongemerkt wegsluizen van informatie.

Vergelijking met een fysieke inbraak

In deze fase overhandigt de inbreker uw kroonjuwelen aan zijn handlanger via het openstaande raam waarlangs hij is binnengekomen of via een eerder opengezette achterdeur.

In deze fase sluizen aanvallers de informatie weg waar zij op uit waren via de verkregen toegang of via het communicatiekanaal met de C2-server. Bij cyberspionage wordt bedrijfs- of overheidsgevoelige informatie van uw organisatienetwerk overgeheveld naar het systeem van de aanvaller. In deze fase wordt steeds vaker niet alleen informatie gestolen die interessant is voor het land waar de opdracht vandaan komt, maar wordt ook andere informatie (bijvangst) buitgemaakt. Statelijke aanvallers maken bij hun cyberaanvallen regelmatig gebruik van ingehuurde hackers, die buitgemaakte bijvangst online op zwarte markten te koop aanbieden. Ook kunnen aanvallers in deze fase overgaan tot het saboteren van systemen of het aantasten van de integriteit van uw data.

Advies – wat kunt u doen?

De aanvallers hebben in deze fase het uiteindelijke doel bereikt. Net als in fase 6 zullen de aanvallers vaak gebruikmaken van reguliere datastromen, dit keer om ongemerkt informatie weg te sluizen uit uw organisatie. De beveiligingsmaatregelen in deze fase zijn daarom gericht op het ontdekken van data exfiltratie en het beperken van eventuele schade.

Preventieve beveiligingsmaatregelen

- U kunt besmette systemen het best isoleren om verdere besmetting te voorkomen. Bij het opschonen van de systemen is het belangrijk dat de aanvaller niet meer op het betreffende systeem aanwezig is en dat alle besmette systemen geschoond worden. U kunt overwegen om nieuwe en ongebruikte systemen in te zetten. Het herstellen van een schone en geverifieerde back-up is de effectiefste manier om zo snel mogelijk de geraakte functionaliteiten weer beschikbaar te stellen. Houd er bij het isoleren van systemen rekening mee dat aanvallers zeer waarschijnlijk opnieuw zullen proberen het netwerk binnen te dringen.

- Een goed incident respons-proces is nodig om onderzoek naar een incident te kunnen doen, maar ook om te bepalen welke stappen u als eerst zet. Voordat u de ‘oude’ situatie kunt herstellen, is het belangrijk dat u vaststelt hoe de aanval is ontstaan en welke informatie de aanvaller heeft buitgemaakt. Daarbij kunt u gebruikmaken van onafhankelijke organisaties die gespecialiseerd zijn in digitaal forensisch onderzoek. Binnen uw organisatie moet u daarnaast duidelijke processen opstellen en duidelijke verantwoordelijkheden afspreken om adequaat te kunnen reageren. Oefen periodiek een dergelijke crisissituatie binnen de organisatie.

- Als uw organisatie een vitale rol heeft in de maatschappij, wordt aangeraden om deze vitale ICT-functionaliteiten binnen een apart geïsoleerd netwerk te plaatsen ten opzichte

van het kantoorautomatiseringsnetwerk. Veilige koppelingen kunnen het mogelijk maken om informatie tussen de netwerken uit te wisselen. Zeker in het geval van vitale processen is het (laten) inrichten van een SOC en een Computer Emergency Response Team (CERT) van cruciaal belang om adequaat te kunnen reageren. Zo kunt u direct handelen en beperkt u eventuele schade.

Detectieve beveiligingsmaatregelen

- Met Data Loss Prevention (DLP) voorkomt u dat gevoelige of vertrouwelijke data onbedoeld terechtkomt bij personen buiten de organisatie. Hiermee kunt u data die de organisatie dreigt te verlaten ontdekken en deze datastromen op tijd blokkeren. Aanvullend kunnen er beveiligingsmaatregelen gekozen worden die voorkomen dat deze data bekeken kan worden. Denk hierbij aan het versleutelen van data.

- Als u in deze fase aanvallers ontdekt, is het belangrijk om te bedenken of u direct mitigerende maatregelen neemt. Als aanvallers weten dat ze ontdekt zijn, kunnen ze besluiten om tegenacties te nemen. Denk hierbij aan het systeem saboteren, sporen wissen of maatregelen die forensisch onderzoek onmogelijk maken. Afhankelijk van uw gekozen beveiligingsmaatregelen en de mogelijke impact van de aanval, kan besloten worden om direct in te grijpen of hiermee te wachten tot een later moment. Laat u bij het maken van deze afweging adviseren door uw SOC, CERT of externe partij die gespecialiseerd is in forensisch onderzoek.

Te koop op een online platform: toegang tot vertrouwelijke bedrijfsnetwerken

Het is voorjaar 2020 als de AIVD ziet dat toegang tot vertrouwelijke netwerken van grote bedrijven en overheidsorganisaties te koop wordt aangeboden op een online forum. Door onderzoek te doen concludeert de AIVD dat deze verkoopadvertenties serieus genomen moeten worden. Waarschijnlijk heeft een professionele hacker deze bedrijven geïnfiltreerd, waarbij hij in veel gevallen de hele Cyber Kill Chain heeft kunnen doorlopen, zonder opgemerkt te worden.

De AIVD weet dat deze hacker regelmatig opdrachten uitvoert voor een buitenlandse inlichtingendienst. Hij lijkt zijn buit altijd eerst tegen betaling aan deze dienst aan te bieden. Als deze geen interesse heeft, wordt de buit te koop aangeboden aan de hoogste bieder. De koper kan vervolgens zelf de plek van de hacker in het netwerk van de bedrijven of overheidsinstanties overnemen en naar eigen inzicht acties uitvoeren (Actions on Objectives), zoals het stelen van (staatsgeheime) informatie en het versleutelen of wissen van digitale systemen.

Deze publicatie is een gezamenlijke uitgave van:

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Algemene Inlichtingen- en Veiligheidsdienst

en

Ministerie van Defensie
Militaire Inlichtingen- en Veiligheidsdienst

juni 2021