Overzicht gevallen waarin het NCSC in ruimere zin dan wettelijk mogelijk informatie heeft gedeeld

In onderstaande gevallen heeft het Nationaal Cyber Security Centrum (NCSC) in ruimere zin dan wettelijk mogelijk informatie gedeeld met schakelorganisaties of individuele andere aanbieders. In de meeste gevallen informeert het NCSC in het geval van een individuele andere aanbieder door het versturen van een e-mail naar het publiek bekende abuse-e-mailadres van een organisatie waarnaar bijvoorbeeld het IP-adres herleidbaar is, of in het geval van een schakelorganisatie, naar het functionele e-mailadres van deze schakelorganisatie dat bekend is bij het NCSC. Deze e-mail bevat de betreffende gegevens, zoals informatie over de geconstateerde kwetsbaarheid, het bijbehorende IP-adres en andere relevante dreigingsinformatie. Daarnaast voegt het NCSC voor zover mogelijk handelingsperspectief toe, bijvoorbeeld een link naar het algemene beveiligingsadvies dat het NCSC heeft gepubliceerd. In enkele van deze gevallen is telefonisch contact gezocht met een organisatie om de informatie snel over te dragen, bijvoorbeeld bij een op handen zijnde ransomware-aanval.

Het NCSC heeft in deze gevallen de informatie beperkt tot de informatie die noodzakelijk is om de aanbieder de directe dreiging weg te kunnen laten nemen. Het ging hierbij bijvoorbeeld om gegevens die het systeem omschrijven, zoals naam van het softwareproduct, IP-adres en poortnummer. Bij een (op handen zijnde) aanval, bijvoorbeeld van ransomware, maakt deze informatie het mogelijk om het besmette systeem of systemen te vinden of om een aanval af te wenden. In de hieronder opgenomen kolom 'soort gegevens' is alleen de informatie vermeld die ruimer dan wettelijk mogelijk is gedeeld.

Casus	Datum	Beschrijving	Verstrekking aan	Soort gegevens
Wereldwijde grootschalige ransomware-aanvallen voorkomen (LockerGoga)	2 mei 2019	Het NCSC heeft samen met partners de infrastructuur blootgelegd van een grootschalige ransomware-campagne. Deze organisatie richtte zich op agressieve ontwrichting van vitale doelwitten door verwoestende ransomware aanvallen op de kritieke infrastructuur, zoals overheidsorganisaties en multinationals over de hele wereld. Vanuit dit onderzoek beschikt het NCSC over concrete informatie over besmettingen. Om grootschalige ransomware-aanvallen, en daarmee grote schade, te voorkomen heeft het NCSC slachtoffers geinformeerd.	Nationaal: - OKTT's[1] en internettoegangsdiensten Internationaal: Ten aanzien van CERT's buiten de EU: - landen die onderdeel uitmaken van het International Watch and Warning Network (IWWN).	IP-adressen, gebruikersnaam
Ernstige kwetsbaarheid in Pulse-secure-software (I)	22 augustus 2019	Er is een ernstige kwetsbaarheid aangetroffen in Pulse-VPN producten. Pulse-VPN is een product waarmee gebruikers op afstand verbinding kunnen maken hun bedrijfsnetwerk en vertrouwelijk kunnen communiceren. Van de kwetsbaarheid wordt actief misbruik gemaakt, waardoor kwaadwillenden	- OKTT's - Enkele (publieke) organisaties zijn rechtstreeks geïnformeerd, waaronder een ambulancedienst en een veiligheidsregio.	IP-adressen

[1] Organisaties die objectief kenbaar tot taak hebben om andere organisaties of het publiek te informeren over digitale dreigingen en incidenten.

Casus	Datum	Beschrijving	Verstrekking aan	Soort gegevens
		gevoelige informatie kunnen stelen en toegang kunnen krijgen tot het VPN-netwerk.		
Ernstige kwetsbaarheid in Citrix-software	10 januari 2020	Deze casus betreft een ernstige kwetsbaarheid (High/High) in Citrix Netscaler-systemen. Met Citrix-Netscaler kunnen gebruikers (onder andere) op afstand verbinding maken hun bedrijfsnetwerk en vertrouwelijk communiceren. Op de kwetsbaarheid in dit product werd gescand ten behoeve van misbruik. Voor de kwetsbaarheid was op dat moment geen patch beschikbaar. Uit technisch onderzoek van het NCSC is gebleken dat tenminste 2000 systemen in Nederland mogelijk kwetsbaar zijn die buiten de doelgroep van het NCSC liggen.	- OKTT's	IP-adressen
Ernstige kwetsbaarheid in Microsoft Windows RD Gateway Server	31 januari 2020	Deze casus betreft een ernstige kwetsbaarheid (High/High) in Windows RDP. Windows RDP kan worden gebruikt om binnen een bedrijfsnetwerk toegang te verkrijgen tot een computer. Deze kwetsbaarheid kan vanaf het internet worden benaderd. Voor de kwetsbaarheid is een patch beschikbaar. Het NCSC heeft een high/high beveiligingsadvies gepubliceerd. Het NCSC heeft van een samenwerkingspartner een lijst met 350 kwetsbare IP-adressen ontvangen. Dit betreffen organisaties buiten de doelgroep van het NCSC.	- OKTT's	IP-adressen
Op handen zijnde ransomware-aanvallen (I)	5 februari 2020	Het NCSC beschikt over informatie waaruit blijkt dat een groot bedrijf, gelegen buiten de wettelijke doelgroep van het NCSC, met ransomware gecompromitteerd is. Dit bedrijf is middels infrastructuur verbonden met diverse doelgroeporganisaties van het NCSC.	- De betreffende organisatie is rechtstreeks geïnformeerd.	Gegevens over de compromittatie zijn met het bedrijf gedeeld.

Casus	Datum	Beschrijving	Verstrekking aan	Soort gegevens
Ernstige kwetsbaarheid in Sharepoint	7 februari 2020	Deze casus betreft een ernstige kwetsbaarheid in Microsoft Sharepoint. Sharepoint wordt o.a. gebruikt om bestanden onderling te delen. Er wordt actief misbruik van deze kwetsbaarheid gemaakt. Het NCSC beschikt over 901-IP-adressen die kwetsbaar zijn voor misbruik. De impact voor een kwetsbaar system kan zeer groot zijn en kan leiden tot uitlekken van gevoelige informatie.	- OKTT's	IP-adressen
Ernstige kwetsbaarheid in Microsoft Windows RDP	18 februari 2020	Het NCSC heeft van een samenwerkingspartner informatie ontvangen over mogelijk gecompromitteerde accounts van Windows RDP. Windows RDP kan worden gebruikt om binnen een bedrijfsnetwerk toegang te verkrijgen tot een computer.	- OKTT's	Computernamen, gebruikersnamen, IP-adressen
Ernstige kwetsbaarheid in Microsoft Exchange	3 maart 2020	Deze casus betreft een ernstige kwetsbaarheid (high/high) in Microsoft Exchange Server. Microsoft Exchange wordt gebruikt voor het beheren van e-mailservers en agendadiensten binnen organisaties. Bij succesvol misbruik van deze kwetsbaarheid kan een kwaadwillende tot het hart van een systeem doordringen. Het NCSC heeft onder andere uit eigen technisch onderzoek gegevens van circa 450 potentieel kwetsbare systemen in bezit die behoren tot achterban van internet-toegangsdiensten en OKTT's.	- OKTT's en internettoegangsdiensten	IP-adressen
Ernstige kwetsbaarheid in Sophos Firewalls	1 mei 2020	Betreft een ernstige kwetsbaarheid (high/high) in Sophos Firewalls. Sophos Firewalls wordt gebruikt om verkeerd vanuit de buitenwereld te scheiden van intern verkeer. Met de kwetsbaarheid kan de firewall worden binnengedrongen en kan het systeem worden overgenomen. De kwetsbaarheid wordt in de praktijk misbruikt. Het NCSC heeft een high/ high beveiligingsadvies uitgebracht.	- internettoegangsdiensten	IP-adressen
Besmette Nederlandse systemen in omvangrijk botnet (Emotet) (I)	20 mei 2020	Het NCSC heeft van een samenwerkingspartner een lijst ontvangen van IP-adressen die besmet zijn met het emotet-botnet (malware). Emotet wordt gebruikt	- internettoegangsdiensten	IP-adressen

Casus	Datum	Beschrijving	Verstrekking aan	Soort gegevens
		voor het versturen van spam en installeren van malware. Het botnet kan worden gebruikt tegen de Nederlandse (vitale) infrastructuur. Het NCSC beschikt over gegevens waaruit blijkt dat klanten van Nederlandse internettoegangsdiensten zijn gecompromitteerd.		
Ernstige kwetsbaarheid in PanOS	2 juli 2020	Er is een ernstige kwetsbaarheid in PanOS, waarmee toegang verkregen kan worden tot het netwerk en de beheerinfrastructuur met admin-rechten. Het NCSC heeft informatie over mogelijk kwetsbare systemen.	-OKTT's. -Daarnaast is een organisatie rechtstreeks geïnformeerd (een veiligheidsregio).	IP-adressen
Ernstige kwetsbaarheid in Solarwinds Orion	30 december 2020 & 7 januari 2021	Er is een versie van SolarWinds Orion verspreid met daarin een moedwillige kwetsbaarheid. SolarWinds Orion is een platform waarmee netwerken worden beveiligd en gemonitord. Volgens Microsoft is de kwetsbaarheid opzettelijk gecreëerd door een statelijke actor. Deze kwetsbaarheid kan door kwaadwillenden worden misbruikt om toegang te krijgen tot systemen. De VS heeft bekend gemaakt dat bij overheidsinstellingen in de Verenigde Staten misbruik is geconstateerd en sprake is van een ernstig incident. Het NCSC heeft een lijst ontvangen van kwetsbare IP-adressen. In januari 2021 heeft het NCSC vervolgens een aanvullende lijst ontvangen met kwetsbare systemen.	- Organisaties zijn rechtstreeks geïnformeerd.	IP-adressen
Melding gecompromitteerd bedrijf	18 januari 2021	Het NCSC heeft van een buitenlandse partner informatie ontvangen dat een IP-adres, op naam van een bedrijf gecompromitteerd is en dat dit IP-adres actief wordt misbruikt. Het risico bestaat dat de malware en daarbij de compromittatie verder wordt verspreid.	-De betreffende organisatie is rechtstreeks geïnformeerd.	IP-adres
Besmette Nederlandse systemen in omvangrijk botnet (Emotet) (II)	3 februari 2021	Het NCSC heeft van een samenwerkingspartner informatie ontvangen van Nederlandse domeinen die besmet zijn het emotet-botnet (malware). Dat zijn in bijna alle gevallen gecompromitteerde systemen die onderdeel zijn van het botnet Emotet. Dit botnet wordt gebruikt voor het versturen van spam en installeren van malware. Het botnet kan worden gebruikt tegen de Nederlandse (vitale) infrastructuur.	-OKTT's -Een organisatie (politieke partij) is rechtstreeks geïnformeerd.	IP-adressen, e-mailadressen

Casus	Datum	Beschrijving	Verstrekking aan	Soort gegevens
Ernstige kwetsbaarheid in Microsoft Windows RDP	23 april 2021	Het NCSC heeft informatie ontvangen over een database met gelekte inloggegevens op Windows RDP. Windows RDP kan worden gebruikt om binnen een bedrijfsnetwerk toegang te verkrijgen tot een computer. De database bevat Nederlandse inloggegevens. Criminelen gebruiken de gecompromitteerde gegevens om zich toegang te verschaffen tot systemen. Zo zijn de inloggegevens van een gemeente die een ransomwareaanval heeft ondervonden, teruggevonden in deze set.	- OKTT's en internettoegangsdiensten	IP-adres, gebruikersnaam, laatste 4 cijfers van wachtwoord
Ernstige kwetsbaarheid in Pulse-secure-software (II)	30 april 2021	Het NCSC heeft informatie ontvangen van een samenwerkingspartner over verhoogde activiteit van malafide verkeer bij VPN-servers van Pulse Secure. Pulse-VPN is een product waarmee gebruikers op afstand verbinding kunnen maken hun bedrijfsnetwerk en vertrouwelijk kunnen communiceren. Met de kwetsbaarheid kunnen kwaadwillenden toegang krijgen tot het systeem. Er is nog geen patch beschikbaar. Uit technisch onderzoek van het NCSC is gebleken dat er Nederlandse servers kwetsbaar zijn die vallen binnen de achterban van OKTT's.	- OKTT's en internettoegangsdiensten	IP-adressen
Ernstige kwetsbaarheid in Exim	10 mei 2021	Het NCSC heeft een high/high beveiligingsadvies uitgebracht voor kwetsbaarheden in Exim. Exim maakt de afhandeling van mails mogelijk. Uit het technisch onderzoek van het NCSC blijkt een groot aantal Exim mailservers in Nederland mogelijk kwetsbaar.	- OKTT's - Vier organisaties zijn rechtstreeks geïnformeerd: twee politieke partijen, een provincie en een veiligheidsregio.	IP-adressen
Ernstige kwetsbaarheid in Sonicwall	15 juli 2021	Vanuit een buitenlandse partner heeft het NCSC een lijst ontvangen met gelekte inloggegevens van VPN-apparatuur. VPN-apparatuur wordt gebruikt om vertrouwelijk te kunnen communiceren. Volgens de partner zijn deze inloggegevens verkregen door een criminele actorgroep die zich primair richt op ransomwareaanvallen. De verwachting is dat deze gegevens ook met dit doel zijn achterhaald. In het betreffende land zijn al organisaties slachtoffer geworden van deze criminale organisatie.	- OKTT's	IP-adres, gebrukersnaam
Gecompromitteerde systemen in Nederland die gebruikt worden bij	28 juli 2021	Het NCSC heeft van een buitenlandse partner een hulpverzoek ontvangen. Daaruit blijkt dat een Europese overheid te maken heeft met digitale aanvallen die dit Europese land	- OKTT's	IP-adressen

Casus	Datum	Beschrijving	Verstrekking aan	Soort gegevens
aanvallen op Europese overheid		attribueert aan een statelijke actor. Nederlandse infrastructuur is gecomprimitteerd en wordt (zonder medeweten van de eigenaren van deze systemen) misbruikt voor deze aanvallen.		
Inloggevens van Fortinet VPN-systemen (1)	9 september 2021	Het NCSC heeft informatie ontvangen over een gepubliceerde lijst met valide inloggegevens voor Fortinet VPN-systemen die in het verleden (2018) via bekende kwetsbaarheden zijn verkregen. Hiermee kan toegang worden verkregen tot systemen. VPN-systemen kunnen worden gebruikt voor vertrouwelijke communicatie.	- OKTT's	IP-adressen, computernaam
Op handen zijnde ransomware-aanvallen (II)	24 september 2021	Het NCSC ontving van een Europese partner informatie over twee partijen die besmet zijn met malware. De Europese partner heeft aangegeven dat deze malware wordt gebruikt vlak voordat er ransomware op de systemen wordt uitgerold.	- OKTT - Een organisatie (een scholengemeenschap) is rechtstreeks geïnformeerd	IP-adressen
Ernstige kwetsbaarheid in Apache	8 oktober 2021	Van een samenwerkingspartner heeft het NCSC een lijst met enkele honderden kwetsbare IP-adressen ontvangen over de Apache webserver. Deze server maakt webpagina's beschikbaar. Middels de kwetsbaarheid kan toegang worden verkregen tot gevoelige gegevens.	- OKTT's	IP-adressen
Op handen zijnde ransomware-aanvallen (III)	19 oktober 2021	Het NCSC heeft van een buitenlandse partner IP-adressen ontvangen van slachtoffers die mogelijk op het punt staan getroffen te worden door een ransomware-aanval.	- OKTT	IP-adressen
Nederlandse systemen die besmet zijn met STRAT-malware	19 oktober 2021	Het NCSC is door een samenwerkingspartner geïnformeerd over STRAT-malware infecties. Ondanks dat de malware nu niet meer actief is, zou het mogelijk kunnen dat deze in het verleden wel actief is geweest en toegang heeft gehad tot wachtwoorden en bestanden.	- OKTT's	IP-adressen
Gecompromitteerde en kwetsbare Fortinet systemen	4 november 2021	Het NCSC heeft een lijst ontvangen van een samenwerkingspartner omtrent kwetsbare en gecompromitteerde Fortinet servers binnen Nederland.	- OKTT's	IP-adressen
Op handen zijnde ransomware-aanvalen (IV)	5 november 2021	Het NCSC heeft van een samenwerkingspartner informatie ontvangen van slachtoffers die mogelijk op	- OKTT's	IP-adressen

Casus	Datum	Beschrijving	Verstrekking aan	Soort gegevens
		het punt staan getroffen te worden door een ransomware-aanval.		
Ernstige kwetsbaarheid in Log4J	23 december 2021	Het NCSC heeft informatie over vermoedelijk kwetsbare systemen voor de Log4j-kwetsbaarheid. Wanneer de kwetsbaarheid wordt misbruikt is er een gerede kans dat de gevolgschade groot is voor de getroffen organisatie zoals uitval van kritieke bedrijfsprocessen.	- OKTT's	IP-adressen
Ernstige kwetsbaarheid in Redis	29 maart 2022	Kwetsbaarheid in Redis-software. Uit technisch onderzoek van het NCSC is gebleken dat in Nederland systemen kwetsbaar zijn voor misbruik. Redis is een veelgebruikt product voor sessiebeheer. Deze kwetsbaarheid kan dienen als springplank om dieper in systemen binnen te dringen ten behoeve van misbruik (voor bijvoorbeeld een ransomware-aanval). Er een exploitcode beschikbaar is en het NCSC ziet dat er door (kwaadwillenden) actief gescand wordt naar deze kwetsbaarheid.	- Hostingproviders zijn rechtstreeks geïnformeerd.	IP-adressen