Analyse DWR 2.0

5.1.2.e

senior adviseurs Privacy Company

Datum: 19 september 2025

Samenvatting

Dit rapport bevat de analyse van technisch onderzoek naar de uitgaande verkeersstromen van de nieuwe digitale werkplek voor Rijksambtenaren. Het onderzoek is begin augustus 2025 afgerond. Daarna heeft overleg plaatsgevonden met SSC-ICT en SLM Rijk, en is het rapport aangepast met aanvullende informatie van SSC-ICT.

Aanleiding

De Tweede Kamer heeft op 27 maart 2025 aan de staatsecretaris van BZK gevraagd om onderzoek te doen of de nieuwe digitale Werkplek Rijk 2.0 (DWR 2.0) data lekt naar externen. De uitvoeringsorganisatie SSC-ICT heeft vervolgens samenwerking gezocht met Strategisch Leveranciersmanagement Microsoft, Google Cloud en AWS (SLM Rijk).

Opzet onderzoek

Omdat medewerkers mogen kiezen tussen een PC met Windows 11 of een Mac met macOS, is er twee keer onderzoek gedaan.

DWR 2.0 maakt gebruik van Netskope, een beveiligde tunnel tussen de werkplek en de buitenwereld. SSC-ICT beheert lokaal een eigen Netskope server. Omdat Netskope een deel van het uitgaande verkeer van de werkplekken eerst naar die lokale Netskope server leidt, is het minder zinvol om het verkeer af te tappen. De werkelijke eindpunten/bestemmingen van het versleutelde verkeer zijn dan niet zichtbaar. Daarom is ook getest zonder Netskope, om te zien welke gegevens er naar externe partijen worden gestuurd zonder dat Netskope het onderscheppen verhindert.

Uitkomsten onderzoek

De belangrijkste bevinding van het technisch onderzoek is dat er maar weinig data uitlekken, dankzij een strakke configuratie van de werkplek, in lijn met de adviezen van SLM Rijk voor een privacyvriendelijke configuratie. Noch Windows noch Office noch Webex sturen onverwachte data uit.

De waargenomen datastroom is beperkt tot noodzakelijke telemetrieberichten om de diensten goed-werkend, veilig en up-to-date te houden, en de Rijksoverheid heeft strakke verwerkersovereenkomsten gesloten voor het gebruik van Microsoft 365 en van Webex. Microsoft en Cisco bieden aan (voor de diensten waarvoor ze verwerker zijn) om vrijwel alle soorten persoonsgegevens te verwerken en op te slaan binnen de EU (Cisco doet dat vanaf eind 2025). Het gaat dan niet alleen om de inhoudelijke gegevens, maar ook om de diagnostische gegevens over het gebruik van de diensten, de support gegevens, de account gegevens en de website gegevens (als je de diensten via de browser wilt gebruiken, en niet als geïnstalleerde app). De Rijksoverheid heeft nog geen afspraken met Apple over MacOS of met Microsoft over Windows 11. Op dit moment is Microsoft geen verwerker voor het besturingssysteem, maar er lopen

gesprekken met SLM Rijk. Microsoft biedt wel de mogelijkheid om de telemetriestroom uit Windows in te zien, en uit te zetten. De Rijksoverheid heeft ook geen afspraken kunnen maken met de makers van browsers, in dit geval Edge en Safari, terwijl die browsers wel informatie kunnen lekken naar de makers. Bij de browser Edge is de default zoekmachine Bing van Microsoft, en bij Safari is de default zoekmachine Google Search. Google en Microsoft zijn zelfstandige verantwoordelijken voor hun zoekmachines. Het Rijk zou ook standaard kunnen kiezen voor een andere privacyvriendelijkere zoekmachine, zoals Ecosia, Qwant, DuckDuckGo of in de nabije toekomst, www.eu-searchperspective.com.

Uitzonderingen

In de eerste plaats kan surfgedrag uitlekken naar derde partijen via **cookies**. Ook met testen met Netskope aan, biedt DWR 2.0 onvoldoende bescherming tegen tracking cookies als ambtenaren websites bezoeken met hun Edge of Safari browser. Het uitgaande verkeer (na het bezoeken van vier websites, met wat doorklikken) bevatte verkeer naar allerlei advertentienetwerken en tracking partijen, zoals Google (met YouTube en DoubleClick), Facebook, Criteo, AdNexus, Hotjar, Adhese, Scorecardresearch, Amplitude en Weborama. Er was ook ander verkeer naar Amerikaanse hosting partijen zoals AWS en naar de content delivery netwerken van Akamai en Cloudflare. In vergelijking tussen de twee besturingssystemen waren er aanzienlijk minder cookies op MacOS. Dat kan twee oorzaken hebben: ofwel het was moeilijker om dit verkeer goed te onderscheppen door ingebouwde privacybescherming in MacOS, of de Safari browser was beter ingesteld. SSC-ICT kan het tracking-risico oplossen door de Edge browser strakker te configureren, en door op beide systemen een extensie zoals uBlock standaard mee te leveren, of een ad-blocking proxy te gebruiken.

In de tweede plaats kan surfgedrag uitlekken via **DNS-verkeer**. Het domeinnaam systeem (DNS) is het telefoonboek van Internet. Iedere keer dat iemand een website bezoekt, gaat er verkeer naar een DNS-server die de domeinnamen vertaalt in IP-adressen. Tijdens het testen is alleen DNS-verkeer geobserveerd naar een DNS-resolver op het lokale netwerk. Op een vertrouwd netwerk vormt dit verkeer geen ongebruikelijk risico. Maar op onvertrouwde netwerken, bij medewerkers thuis, of onderweg in hotels of cafés, kan dat betekenen dat de domeinnamen waarmee de medewerker verbinding maakt uitlekken. Het is normaal dat een beheerder van een netwerk DNS-verkeer kan inzien, maar als met Netskope het netwerkverkeer wordt afgeschermd voor het geval er op onvertrouwde netwerken wordt gewerkt, is het verstandig om dat ook met DNS-verzoeken te doen. Netskope heeft opties om ook DNS-verkeer te beschermen. SCC-ICT zou deze optie kunnen onderzoeken.

In de derde plaats heeft Privacy Company verkeer waargenomen naar de **Windows Store**, hoewel de Windows Store uitstaat voor medewerkers. Het verkeer komt omdat Microsoft via de Windows Store allerlei updates binnenhaalt voor allerlei interne Windows componenten en software. Via de telemetrie (op het niveau 'Required' verzamelt Microsoft (als verantwoordelijke) informatie over updates van de Windows camera, Windows To Do, Paint, Notepad, Screensketch, de Desktop app installer en Windows alarms. De waargenomen telemetrie ging ook over updates van HP Audio Control en HP system information, en over

de (externe) Display link manager software. Een typisch Windows-telemetriebericht bevat een uniek nummer, een tijdstempel, verschillende unieke identificatiegegevens voor de eindgebruiker en het apparaat, en verschillende stukjes informatie over bijvoorbeeld het type apparaat, de schermgrootte, het besturingssysteem, de software en/of het stuurprogramma. Omdat Microsoft voor deze telemetrie optreedt als verantwoordelijke, kan zij die informatie voor haar eigen doelen verwerken, inclusief commerciële doelen en (buiten Windows en Office om) het tonen van gerichte advertenties. Microsoft waarschuwt dat organisaties de telemetrie weliswaar kunnen uitzetten (niveau Security), maar dat Microsoft dan geen informatie kan verzamelen over mislukte updates. SSC-ICT zou niettemin de optie kunnen onderzoeken om de telemetrie uit Windows uit te zetten.

In de vierde plaats heeft Privacy Company twee soorten uitgaand verkeer vanuit Windows waargenomen naar een aantal **semi-lokale IP-adressen** (*carrier-grade NAT*), Windows fileshare en Windows Update Delivery Optimization. Wanneer Windows zoekt naar Windows-updates en downloads uit de Microsoft Store, probeert Windows eerst op het lokale netwerk andere computers te vinden die deze bestanden al hebben. Microsoft laat de lokale systemen dus de toegang tot de updates delen om netwerkcapaciteit te besparen. De aangetroffen IP-adressen zijn mogelijk onderdeel van de configuratie bij SSC-ICT, op één opmerkelijke uitzondering na: één van de IP-adressen is eigendom van Mercedes Benz. SSC-ICT heeft met een schermafbeelding aangetoond dat Netskope het verkeer naar dit IP-adres al standaard blokkeerde. Dat klopt ook met de bevinding dat er geen verkeer terugkwam.

In de vijfde plaats is verkeer waargenomen naar **Apple** met de **inhoudelijke zoekopdracht** die een gebruiker had ingevoerd in de Apple zoektool Spotlight. Standaard zoekt Spotlight ook naar online resultaten (websuggesties). SSC-ICT kan dit verkeer verhinderen door het vinkje 'Websites' uit te zetten in de macOS interface. Twee andere aanbevelingen zijn om de widgets uit te zetten en om de optie uit te zetten om Apple te helpen bij het verbeteren van de zoekfunctie. Dit omdat Apple, net als Microsoft voor Windows, een zelfstandige verantwoordelijke is voor alle gegevensverwerkingen via het macOS, en de overheid de datastromen zoveel mogelijk zou moeten minimaliseren.

Tabel 1: Aanbevolen maatregelen SSC-ICT en SLM Rijk

SSC-ICT	SLM RIJK
Overweeg om Firefox Enterprise te installeren als standaard browser, in plaats van Edge. Maak gebruik van de handleiding met privacyvriendelijke instellingen van SLM Rijk.	SLM publiceert dit najaar een vergelijking tussen Edge en Firefox, met privacyvriendelijke configuraties.
Overweeg om een extensie zoals uBlock te installeren om risico op malware via advertenties te verminderen.	
Overweeg om als standaard zoekmachine Ecosia, Qwant, DuckDuckGo of in de toekomst, eu-searchperspective.com te installeren.	
Dwing gebruik van de beveiligde DNS standaard DOH af, maar beperk het DNS-verkeer vanaf de werkplek tot de vertrouwde Rijks DNS-	

servers, zodat verkeer wel versleuteld is voor derde partijen op netwerk, maar wel gemonitord kan worden door de Rijksoverheid.	
Blokkeer al het uitgaand verkeer naar de Windows Update poort 7680 (sta alleen IP-adressen toe binnen het vertrouwde overheidsnetwerk)	Bespreek met Microsoft het privacyrisico van gebruik van de Windows Store voor de Windows updates.
Blijf de privacyvriendelijke configuratie-adviezen volgen voor Microsoft 365 in de handleidingen die SLM Rijk publiceert. Overweeg de voor- en nadelen van het uitzetten van de Windows telemetrie (security).	Versie 3.3 van september 2025 is beschikbaar op: https://slmmicrosoftrijk.nl/?sdm_process_download=1&download_id=13350
Verhinder verkeer naar Apple (als verantwoordelijke) door drie opties uit te zetten: Websites, Widgets en de optie om Apple te helpen bij het verbeteren van de zoekfunctie.	

Begrippenlijst

Term	Uitleg
Carrier-grade NAT	Een oplossing voor een tekort aan IPv4 adressen waardoor verschillende internetproviders IP-adressen kunnen hergebruiken.
CDN	Content Delivery Network, een geografisch verspreid netwerk van proxy-servers om een kopie van informatie zo dicht mogelijk bij de gebruiker te bewaren.
DNS	Domain Name System, dit systeem zorgt o.a voor de vertaling van (leesbare) domeinnamen zoals www.rijksoverheid.nl naar een IP-adres.
HTTP	Hyper Tekst Transfer Protocol, het protocol waarmee voornamelijk documenten op het web worden uitgewisseld (zie ook HTTPS).
HTTPS	HTTP over een beveiligde ("Secure") verbinding. Tegenwoordig is dat voornamelijk HTTP over TLS.
RTP	Real-time Transport Protocol, een protocol ontworpen om audio en video streams over het internet te versturen, bijvoorbeeld voor videoconferencing.
Telemetrie	Gegevens die automatisch vanuit een applicatie of browser naar de maker ervan worden verstuurd. Het gaat hier om een eenzijdige, extra gegevensstroom bovenop de reguliere tweewegscommunicatie via internet.
TLS	Transport Layer Security, een protocol waarmee internetverbindingen kunnen worden versleuteld en kan worden geverifieerd of er met het juiste systeem wordt gecommuniceerd.
VPN	Virtual Private Network. Een VPN zorgt voor een beveiligde en versleutelde verbinding tussen de gebruiker en internet.
WUDO	Windows Update Delivery Optimization, een protocol dat Microsoft gebruikt om computers in een lokaal netwerk Windows- en Microsoft Store-apps en updates in de cache op te slaan en te delen.
XMPP	Extensible Messaging and Presence Protocol, een protocol voor berichtenuitwisseling voor bijvoorbeeld online chat of het versturen van pushberichten.

1. Inleiding

De Tweede Kamer heeft op 27 maart 2025 aan de staatsecretaris van BZK gevraagd om onderzoek te doen of de nieuwe digitale Werkplek Rijk 2.0 (DWR 2.0) data lekt naar externen.[1] De uitvoeringsorganisatie SSC-ICT heeft vervolgens samenwerking gezocht met Strategisch Leveranciersmanagement Microsoft, Google Cloud en AWS (SLM Rijk).

Omdat medewerkers mogen kiezen tussen een PC met Windows 11 of een Mac met MacOS, is er twee keer onderzoek gedaan, op beide systemen.

SSC-ICT gaf aan de nieuwe Digitale Werkplek Rijk 2.0 uit de volgende componenten bestaat:

1. Intune
2. Defender for endpoint
3. Office 365
4. Windows 11
5. Teams (fase1)
6. Webex
7. Exchange on-prem, maar wel met een online koppeling
8. Netskope

Privacy Company heeft de vraag van de Tweede Kamer in overleg met SSC-ICT en SLM Rijk vertaald in de volgende drie onderzoeksvragen.

1. Of SSC-ICT de relevante privacyvriendelijke configuratie-adviezen van de SLM Rijk Handleiding privacyvriendelijke instellingen Microsoft 365 - V2 - 20231114 heeft doorgevoerd (voor zover relevant).[2]

2. Breng in kaart naar welke externe servers de werkplek communiceert, via welk netwerkprotocol of poort. Geef per server de volgende informatie:

    a. IP-adres en/of domeinnaam
    b. Gebruikte netwerkprotocollen of poorten
    c. De hoeveelheid geobserveerde data of het aantal requests
    d. De eigenaar van het block IP-adressen of de domeinnaam op basis van WHOIS informatie
    e. Waar beschikbaar, informatie over het proces dat verbinding maakt

[1] Brief aan de staatssecretaris BZK d.d. 27 maart 2025 inzake verzoek om in de beperkte pilot van de Digitale Werkplek Rijk 2.0 ook te onderzoeken of en hoeveel data er lekt naar externen, middels een onderzoek zoals in 2020 uitgevoerd door de Privacy Company op verzoek van het Ministerie van Justitie en Veiligheid, URL: https://www.tweedekamer.nl/kamerstukken/detail?id=2025Z05916&did=2025D13056.

[2] SLM Rijk heeft in juli 2025 een update (v3) van deze handleiding gepubliceerd, o.a. met relevante instellingen voor Windows 11 en Copilot. URL: https://slmmicrosoftrijk.nl/?sdm_process_download=1&download_id=13350.

f. Waar mogelijk een korte omschrijving van het verkeer op basis van de inhoud, context en/of ervaring van Privacy Company
g. Waar relevant, opmerkingen over maatregelen of architectuur die het lastiger te maken om de inhoud van het verkeer in te zien

3. Geef een uitgebreidere analyse over de inhoud van geobserveerde gegevensstromen, als het verkeer privacyvraagtekens oproept. Ga daarbij in ieder geval in op de volgende elementen:

    1. Het gebruik van cookies
    2. Telemetrie / Required Service Data

2. Testmethodiek

Privacy Company heeft twee varianten van DWR 2.0 getest: op een Macbook met macOS (15.5) en op een Windows 11 laptop, versie 24H2.

DWR 2.0 maakt gebruik van Netskope, een beveiligde tunnel tussen de werkplek en de buitenwereld. SSC-ICT beheert lokaal een eigen Netskope server. Omdat Netskope een deel van het uitgaande verkeer van de werkplekken eerst naar die lokale Netskope server leidt, is het minder zinvol om het verkeer af te tappen. De werkelijke eindpunten/bestemmingen van het versleutelde verkeer zijn dan niet zichtbaar. Daarom is ook getest zonder Netskope, om te zien welke gegevens er naar externe partijen worden gestuurd zonder dat Netskope het onderscheppen verhindert.

Tijdens de test met Netskope is al het uitgaande netwerkverkeer met de tool Wireshark onderschept en vastgelegd. Wireshark analyseert de bestemmingen (IP-adressen) van verkeer, maar kan niet in de versleutelde inhoud kijken. Met Wireshark is dus alleen verkeer vastgelegd dat niet met Netskope werd versleuteld, zoals cookie verkeer.

Daarom is dezelfde test herhaald zonder Netskope. Normale gebruikersaccounts hebben geen rechten om Netskope uit te schakelen, maar de test-accounts zijn voor deze test van extra rechten voorzien.

Tijdens de test zonder Netskope is de werkplek geconfigureerd met mitmproxy (versie 11.0.2) als proxy om de inhoud van zoveel mogelijk versleuteld netwerkverkeer inzichtelijk te maken. Mitmproxy is geconfigureerd om het langskomende netwerkverkeer op te slaan zonder verdere aanpassingen. Het certificaat van mitmproxy is als vertrouwd certificaat toegevoegd aan de vertrouwde certificaten-autoriteit in de twee geteste besturingssystemen.

Dat heeft geresulteerd in vier variaties van de tests:

1. Windows 11 met Netskope ingeschakeld
2. Windows 11 met Netskope uitgeschakeld

3. macOS met Netskope ingeschakeld
4. macOS met Netskope uitgeschakeld

Naast Mitmproxy en Wireshark is het gegevensverkeer nog op twee andere manieren onderzocht: door inzage in de netwerklogs van Netskope, en met de ingebouwde telemetrieviewer in Windows. MacOS beschikt niet over zo'n tool.

De netwerklogs die SCC-ICT ter beschikking heeft gesteld waren geen historische log van netwerkverkeer dat langs de Netskope servers is geleid, en boden daarom geen zinvolle aanvulling op de analyse van het onderschepte verkeer. In plaats daarvan bevatten de logs allerlei configuratie en netwerkstatus et cetera op het moment van uitdraaien, inclusief debug logs van applicaties, maar geen historische gegevens over netwerkverbindingen. Daarom zijn deze netwerklogs verder niet geanalyseerd in dit rapport.

Netwerkverkeer naar lokale adressen (10.*.*.*, 192.*.*.* en *.local domeinnamen) is uit de resultaten gefilterd, omdat dit uniek is voor de testopstelling, en niet representatief is, en omdat de achterliggende vraag van deze opdracht was om het verkeer in kaart te brengen dat naar buiten gaat.

De test scenario's waren als volgt:

- In- en uitloggen op de werkplek.
- Het aanmaken en bewerken van verschillende documenten (Excel, Word, Powerpoint, PDF en een jpg).
- Het zoeken naar inhoud van documenten via de in het besturingssysteem ingebouwde zoekmogelijkheden.
- Het versturen en ontvangen van e-mails tussen de twee test-accounts en met een externe test-account.
- Een kort chat en video-overleg tussen de twee accounts met Teams en Webex.
- Het installeren van software voor persoonlijk gebruik via de ingebouwde appstores van de twee besturingssystemen, en het installeren van een applicatie zonder gebruik te maken van die store, voor zover dat technisch is toegestaan vanaf de nieuwe werkplek.
- Het gebruik van een netwerkschijf, voor zover de werkplek daar toegang toe heeft.
- Websites bezoeken met de standaard webbrowser met in ieder geval een nieuws-website (nu.nl), medische website (thuisarts.nl), overheids-website (rijksoverheid.nl) en een website met software die herkenbaar als verdacht wordt aangemerkt (phishing/malware/etc.,eicar.org)
- Het maken van screenshots.

Nota bene

Alle TCP-pakketten bevatten het IP-adres van betrokken Rijkswerknemer. Dat wordt niet bij elke bevinding hieronder herhaald. Bovendien registreert de ontvanger automatisch het tijdstip van ontvangst.

3. Testresultaten

Dit rapport is verdeeld in twee hoofddelen: het eerste deel over de Windows-bevindingen, het tweede deel over de MacOS bevindingen.

3.1 Windows (met en zonder Netskope)

Paragraaf 3.1.1 hieronder groepeert alle eindpunten die op Windows zijn waargenomen naar de (vermoedelijke) gebruiker. De IP-adressen zijn vertaald naar domeinnamen met behulp van WHOIS. Deze lijst bevat ook de domeinnamen van de bewust bezochte websites. Het websitebezoek was verantwoordelijk voor het merendeel van het waargenomen verkeer, inclusief verkeer naar advertentienetwerken, grote webhosting partijen zoals AWS en Content Delivery Networks zoals Akamai en Cloudflare.

Het meeste verkeer is onderschept zonder Netskope, omdat Netskope een tunnel vormt tussen de laptop van de medewerker en de Netskope servers die SCC-ICT lokaal beheert. Het meeste verkeer lijkt daarom alleen naar de Netskope server te gaan. Alleen onversleuteld verkeer kon worden bekeken, zoals verkeer vanuit poort 80. Daarom lijkt het alsof Netskope nauwelijks verkeer doorlaat naar externe partijen in de tabel van paragraaf 0. Maar dat is niet de juiste conclusie: Netskope maakte alleen het onderscheppen van versleuteld verkeer onmogelijk, maar Netskope is niet bedoeld om tracking verkeer tegen te houden.

In paragraaf 3.1.2 is het waargenomen netwerkverkeer uitgesplitst naar protocol, zoals DNS-verkeer, HTTP of specifiek Windows verkeer.

Paragraaf 3.1.3 bevat een tabel met de waargenomen cookies. Die bevat vooral advertentie en tracking analytics cookies die door de bezochte websites zijn geplaatst, met een paar uitzonderingen van cookies die door gebruik van de functionele applicaties zijn geplaatst.

Paragraaf 3.1.4 bevat een overzicht van het verkeer dat is waargenomen met de Diagnostic Data Viewer. Dat is een tool die Microsoft (op verzoek van SLM Rijk) ingebouwd heeft in Windows om telemetrieberichten leesbaar te maken, zowel uit Windows als uit Office 365.

3.1.1 Geobserveerde netwerk-eindpunten (met en zonder Netskope)

3.1.1.1 Adhese (tracker)

ads-dpgmediabe.adhese.com
user-sync.adhese.com

3.1.1.2 Adnexus (tracker)

acdn.adnxs.com
ams3-ib.adnxs.com
cdn.adnxs.com

ib.adnxs.com

3.1.1.3 Akamai (CDN)

a1221.dscd.akamai.net
a1579.d.akamai.net
a1813.dscd.akamai.net
a1817.dscd.akamai.net
a1847.dscg2.akamai.net
a1864.dscd.akamai.net
a1894.dscb.akamai.net
a1961.g2.akamai.net
a1968.i6g1.akamai.net
a360.dscd.akamai.net
a390.dscd.akamai.net
a726.dscd.akamai.net
a937.dscb.akamai.net
a978.i6g1.akamai.net
e10370.d.akamaiedge.net
e119.dsca.akamaiedge.net
e12627.g.akamaiedge.net
e127270.dscd.akamaiedge.net
e184071.dscb.akamaiedge.net
e26769.dscb.akamaiedge.net
e27429.dscb.akamaiedge.net
e28241.dscb.akamaiedge.net
e2867.dsca.akamaiedge.net
e3913.cd.akamaiedge.net
e6603.g.akamaiedge.net
e67691.dscb.akamaiedge.net
e69879.dscb.akamaiedge.net
e77980.dscd.akamaiedge.net
e86303.dscx.akamaiedge.net
eudbipv4.clients.config.office.akadns.net
prodeu.officeenrichment.osi.office.net.akadns.net
prodeu.shredder.osi.office.net.akadns.net
weu.pptsgs.live.com.akadns.net
www.tm.a.prd.aadg.akadns.net
www.tm.f.prd.aadg.akadns.net
www.tm.v4.a.prd.aadg.akadns.net
g2a02-26f0-1180-0035-0000-0000-0210-6ac5.deploy.static.akamaite
a95-101-136-223.deploy.static.akamaitechnologies.com
a23-48-125-217.deploy.static.akamaitechnologies.com
a23-73-0-190.deploy.static.akamaitechnologies.com
a23-38-23-24.deploy.static.akamaitechnologies.com

3.1.1.4 Amazon (hosting en CDN)

ac99c40bc9e28338c.awsglobalaccelerator.com
d162h6x3rxav67.cloudfront.net
d16t1nucl0wcte.cloudfront.net
d2f5rvg67fro0x.cloudfront.net
d2xvo51pr40ne7.cloudfront.net

d3l8kopw1d3uiv.cloudfront.net
d96vky0xjhjcq.cloudfront.net
da-pr-ecslo-16vz8llff1sru-159561671.eu-central-1.elb.amazonaws.
dzfq4ouujrxm8.cloudfront.netsp-20191001060653164200000004-710657394.eu-west-1.elb.amazonaws
qnl-play-fetch.s3.amazonaws.com
qnl-play-fetch.s3.amazonaws.com
s3-3-w.amazonaws.com
s3-3-w.amazonaws.com

3.1.1.5 Amplitude (tracker)

api.eu.amplitude.com
api.lab.eu.amplitude.com
api-sr.eu.amplitude.com
cdn.amplitude.com
sr-client-cfg.eu.amplitude.com

3.1.1.6 BrandMetrics (tracker)

cdn.brandmetrics.com
collector.brandmetrics.com

3.1.1.7 Btloader (CDN)

api.btloader.com
btloader.com

3.1.1.8 Carrier-Grade NAT

3.1.1.9 Casale Media (tracker)

htlb.casalemedia.com
ssum-sec.casalemedia.com

3.1.1.10 Cloudflare

cdn.jsdelivr.net.cdn.cloudflare.net
kit.fontawesome.com.cdn.cloudflare.net

3.1.1.11 Criteo (tracker)

ag.gbc.criteo.com
bidder.criteo.com
dnacdn.net
gbc2.fr3.eu.criteo.com
gbc8.nl3.eu.criteo.com
gem.gbc.criteo.com

gum.criteo.com
gum.nl3.vip.prod.criteo.com
in-ftd-65.nl3.vip.prod.criteo.com

3.1.1.12 DPG Media (nieuws)

c.dpgmedia.net
dmoi.api.dpgmedia.net
images.nu.nl
login.dpgmedia.nl
login.nu.nl
myprivacy-static.dpgmedia.net
pg.nu.nl
www.nu.nl

3.1.1.13 Eicar (test malware)

eicar.org
secure.eicar.org
www.eicar.org

3.1.1.14 Facebook (tracker)

connect.facebook.net
scontent.xx.fbcdn.net
star-mini.c10r.facebook.com
www.facebook.com

3.1.1.15 Fastly (CDN)

5.1.2.h
amplitude.map.fastly.net
jsdelivr.map.fastly.net
linkedin.map.fastly.net
prod.appnexus.map.fastly.net

3.1.1.16 Google (inclusief Doubleclick)

ad.doubleclick.net
adservice.google.com
clients2.google.com
clients2.googleusercontent.com
cm.g.doubleclick.net
dns.google
ep1.adtrafficquality.google
ep1.adtrafficquality.google
ep2.adtrafficquality.google
ep2.adtrafficquality.google
fonts.gstatic.com
googleads.g.doubleclick.net
googlehosted.l.googleusercontent.com
img.youtube.com
img.youtube.com
ogads-pa.clients6.google.com
pagead2.googlesyndication.com

play.google.com
region1.google-analytics.com
www.google.com
www.googletagmanager.com
www.youtube.com
www.youtube.com
youtube-ui.l.google.com
ytimg.l.google.com

3.1.1.17 Hotjar (analytics tracker)

content.hotjar.io
pacman-content-live.live.eks.hotjar.com
script.hotjar.com
static.hotjar.com
static-cdn.hotjar.com
ws.hotjar.com
wsky-live.live.eks.hotjar.com

3.1.1.18 Local Area Network

5.1.2.h

3.1.1.19 Mercedes Benz (zie par. 3.1.2.4)

5.1.2.h

3.1.1.20 Microsoft

Onderstaande lijst bevat veel verkeer naar Microsoft domeinen die in hun naam verwijzen naar Windows, Edge of Office. Maar er is ook verkeer waargenomen, dat meestal niet te onderscheppen viel in leesbare vorm met Mitmproxy naar cloudapp.azure.com. Dat zou veroorzaakt kunnen zijn doordat de bezochte websites onderdelen hosten op het Microsoft Azure platform, maar sommige berichten zijn door Office veroorzaakt. Zie de geel gehighlighte berichten met het woord 'augloop' erin. Microsoft verzamelt via augloop telemetrie informatie over het gebruik van Copilot. Tijdens de tests heeft Privacy Company geen gebruik gemaakt van Copilot, maar omdat het logo van Copilot overal opduikt is het mogelijk dat Microsoft daardoor verkeer naar augloop.office.com heeft verzameld.

a-0019.standard.a-msedge.net
ad.sxp.smartclip.net
AMS-efz.ms-acdc.office.com
amsub0302sfring.northeurope.cloudapp.azure.com
api.diagnostics-eudb.office.com
array501.prod.do.dsp.mp.microsoft.com
array508.prod.do.dsp.mp.microsoft.com
array510.prod.do.dsp.mp.microsoft.com
array512.prod.do.dsp.mp.microsoft.com
array518.prod.do.dsp.mp.microsoft.com
array616.prod.do.dsp.mp.microsoft.com
augloop.office.com
augloop-prod-pa00.westeurope.cloudapp.azure.com
augloop-prod-pd02.westeurope.cloudapp.azure.com
augloop-prod-pd04.westeurope.cloudapp.azure.com
autodiscover-s.outlook.com
ax-0002.ax-dc-msedge.net
ax-0002.ax-msedge.net
beta-autodetect.outlookmobile.com.trafficmanager.net
binaries.templates.cdn.office.net
bx-9999.bx-msedge.net
cdn-eu.readspeaker.com
config.edge.skype.com
config.teams.microsoft.com

default.exp-tas.comwww.tm.a.prd.aadg.trafficmanager.net
disc501.prod.do.dsp.mp.microsoft.com
dual-spo-0005.spo-msedge.net
dwrt1.sharepoint.com
e-0014.e-msedge.net
edge.microsoft.com
edgeassetservice.azureedge.net
edge-consumer-static.azureedge.net
entitlement.diagnostics-eudb.office.com
eop-g2.tm-4.office.com
euc.pptsgs.officeapps.live.com
eu-mobile.events.data.microsoft.com
eu-office.events.data.microsoft.com
europe.smartscreen.microsoft.com
exo.nel.measure.office.net
fd.api.iris.microsoft.com
geo.prod.do.dsp.mp.microsoft.com
global-entry-sts.trafficmanager.net
graph.microsoft.com
incidents.diagnostics-eudb.office.com
iris-de-prod-azsc-v2-frc-b.francecentral.cloudapp.azure.com
iris-de-prod-azsc-v2-neu.northeurope.cloudapp.azure.com
iris-de-prod-azsc-v2-neu-b.northeurope.cloudapp.azure.com
k-9999.k-msedge.net
kv501.prod.do.dsp.mp.microsoft.com
l-0007.l-msedge.net
ln-9999.ln-msedge.net
login.live.com
login.microsoftonline.com
md-prod-simcon-ip0.northeurope.cloudapp.azure.com
md-prod-simcon-ip1.northeurope.cloudapp.azure.com
md-prod-simcon-ip1.westeurope.cloudapp.azure.com
md-prod-simcon-ip128.northeurope.cloudapp.azure.com
md-prod-simcon-ip129.northeurope.cloudapp.azure.com
metadata.templates.cdn.office.net
metrics.mopinion.com
mil30r9a.msedge.net
msedge.b.tlu.dl.delivery.mp.microsoft.com
nleditor.osi.office.net
nmoendpoint.northeurope.cloudapp.azure.com
odc.officeapps.live.com
officeclient.microsoft.com
officewhatsnew.z13.web.core.windows.net
omex.cdn.office.net
onedscolprdfrc00.francecentral.cloudapp.azure.com
onedscolprdfrc07.francecentral.cloudapp.azure.com
onedscolprdgwc06.germanywestcentral.cloudapp.azure.com
onedscolprdneu00.northeurope.cloudapp.azure.com
onedscolprdneu01.northeurope.cloudapp.azure.com
onedscolprdneu03.northeurope.cloudapp.azure.com
onedscolprdneu04.northeurope.cloudapp.azure.com

onedscolprdneu05.northeurope.cloudapp.azure.com
onedscolprdneu06.northeurope.cloudapp.azure.com
onedscolprdneu10.northeurope.cloudapp.azure.com
onedscolprdneu11.northeurope.cloudapp.azure.com
onedscolprdneu12.northeurope.cloudapp.azure.com
onedscolprdneu13.northeurope.cloudapp.azure.com
onedscolprdneu14.northeurope.cloudapp.azure.com
onedscolprdweu01.westeurope.cloudapp.azure.com
onedscolprdweu02.westeurope.cloudapp.azure.com
onedscolprdweu05.westeurope.cloudapp.azure.com
onedscolprdweu06.westeurope.cloudapp.azure.com
onedscolprdweu07.westeurope.cloudapp.azure.com
onedscolprdweu09.westeurope.cloudapp.azure.com
onedscolprdweu11.westeurope.cloudapp.azure.com
onedscolprdweu13.westeurope.cloudapp.azure.com
onedscolprdweu15.westeurope.cloudapp.azure.com
osiprod-frc-bronze-azsc-000.francecentral.cloudapp.azure.com
osiprod-frc-buff-azsc-000.francecentral.cloudapp.azure.com
osiprod-neu-bronze-azsc-000.northeurope.cloudapp.azure.com
osiprod-neu-flax-azsc-000.northeurope.cloudapp.azure.com
osiprod-uks-bronze-azsc-000.uksouth.cloudapp.azure.com
osiprod-weu-bronze-azsc-000.westeurope.cloudapp.azure.com
osiprod-weu-buff-azsc-000.westeurope.cloudapp.azure.com
otelrules.svc.static.microsoft
outlook.office.com
outlook.office365.com
partition-cname-trouter-ic3-edf-trouter-service-trouter-1.d02-0
partition-cname-trouter-ic3-edf-trouter-service-trouter-2.d02-0
pexsucpeu03.swedencentral.cloudapp.azure.com
platform.linkedin.com
prod.rewardsplatform.microsoft.com
prod-4c1.rewardsplatform.microsoft.com
prod-agic-ne-8.northeurope.cloudapp.azure.com
prod-agic-we-4.westeurope.cloudapp.azure.com
prodeu.enrichment.osi.office.net
prod-eu-resolver.naturallanguageeditorservice.osi.office.net.ak
prod-global-autodetect.acompli.net
pub-ent-euno-10-t.trouter.teams.microsoft.com
pub-ent-plce-01-t.trouter.teams.microsoft.com
res.cdn.office.net
roaming-eu.officeapps.live.com
s-0005.dual-s-dc-msedge.net
s-0005.dual-s-msedge.net
s-0005.s-msedge.net
s-0006.s-msedge.net
settings-prod-neu-1.northeurope.cloudapp.azure.com
settings-prod-neu-2.northeurope.cloudapp.azure.com
shredder-eu.osi.office.net
s-part-0039.t-0009.fb-t-msedge.net
s-part-0039.t-0009.t-msedge.net
s-part2-t-9999.fb-t-msedge.net

static.edge.microsoftapp.net
statics.teams.cdn.office.net
substrate.office.com
support.content.office.net
t-9999.fb-t-msedge.net
teams.microsoft.com
uks-azsc-config.officeapps.live.com
wac-9999.wac-msedge.net
waws-prod-fra-037-8717.germanywestcentral.cloudapp.azure.com
web.blz22prdstr01a.store.core.windows.net
westeurope-pd02.augloop.office.com
weu-azsc-config.officeapps.live.com
www.bing.com
www.tm.prd.ags.trafficmanager.net

3.1.1.21 Mopinion (feedback)

survey-cache.mopinion.com
survey-collect.mopinion.com
survey-deploy.mopinion.com

3.1.1.22 Netskope

5.1.2.h
5.1.2.h
5.1.2.h

3.1.1.23 Rijksoverheid

5.1.2.h (SSC-ICT)
minbzk.nl
5.1.2.h
5.1.2.h

5.1.2.h

www.rijksoverheid.nl

3.1.1.24 Thuisarts

stats.thuisarts.nl
www.thuisarts.nl

3.1.1.25 Smartocto (analytics)

api.smartocto.com
ingestion.smartocto.com
tentacles.smartocto.com

3.1.1.26 Webex

avatar-a.wbx2.com
avatar-prod-us-east-2.webexcontent.com
binaries.webex.com
board-a.wbx2.com
calliope-anycast.prod.infra.webex.com
client-upgrade-a.wbx2.com
conv-a.wbx2.com
ds.ciscospark.com
encryption-a.wbx2.com
epx-enterpriseproxy-2.d03-046.ic3-calling-enterpriseproxy.01-we
feature-broadcast-b.wbx2.com
global-nebulab-jfk02-dfw01.webex.com
global-utsa.webex.com
idbroker.webex.com
idbroker-guest-a.wbx2.com
idbroker-guest-k.wbx2.com
join-test.webex.com
llm1-connection-k.wbx2.com
locus-b.wbx2.com
mercury-connection-partition1-a.wbx2.com
metrics-a.wbx2.com
pricing.webex.com
prod-achm-general.svc.webex.com
prod-afra-general.svc.webex.com
proximity-a.wbx2.com
tsa.webex.com
tsa3.webex.com
u2c.svc.webex.com
u2c-a.wbx2.com
wdm-a.wbx2.com
wdm-k.wbx2.com
web.webex.com
www.cisco.com
www.webex.com
www-service-a.wbx2.com

wxt-ci-ingressgateway.acmhwxt-prd-2.prod.infra.webex.com
wxt-ci-ingressgateway.afrawxt-prd-1.prod.infra.webex.com
wxt-general-ingressgateway.acmhwxt-prd-1.prod.infra.webex.com
wxt-general-ingressgateway.acmhwxt-prd-2.prod.infra.webex.com
wxt-general-ingressgateway.afrawxt-prd-2.prod.infra.webex.com
wxt-meet-ingressgateway.apdxwxt-prd-2.prod.infra.webex.com
wxt-mercury-ingressgateway.acmhwxt-prd-2.prod.infra.webex.com
wxt-mercury-ingressgateway.afrawxt-prd-1.prod.infra.webex.com
wxt-message-ingressgateway.acmhwxt-prd-1.prod.infra.webex.com
wxt-registration-ingressgateway.acmhwxt-prd-1.prod.infra.webex.
wxt-registration-ingressgateway.acmhwxt-prd-4.prod.infra.webex.
wxt-registration-ingressgateway.afrawxt-prd-1.prod.infra.webex.
wxt-registration-ingressgateway.afrawxt-prd-2.prod.infra.webex.
wxt-wxid-ingressgateway.acmhwxt-prd-3.prod.infra.webex.com
xlm59.public.wamsm-a-0.prod.infra.webex.com

3.1.1.27 Weborama (tracker)

ade.weborama.nl
mrq.weborama.nl

3.1.1.28 Lijst met hosts waarvan maar 1 domein is gesignaleerd

Tabel 2: Identiteit van host en geobserveerd domein

Identiteit	Domein
Ad Delivery (advertenties)	ad-delivery.net
Bunny.net (CDN)	js-sec.indexww.comrealtime-tentacles-production.b-cdn.net
CCM19 (Cookie Consent Manager)	cloud.ccm19.de
Contentsquare (analytics)	t.contentsquare.net
Digital Audience (advertenties)	target.digitalaudience.io
DNS Finder (onbekend)	ag.dns-finder.com
Echobox (AI marketing/newsletters)	applets.ebxcdn.com
IP data (IP geolocatie)	api.ipdata.co
Jsdeliver (CDN)	cdn.jsdelivr.net
Kantar Media	end.nmo-ep.nl
Onbekend	urbanlaurel.com
Onbekend - DNS finder	ag.dns-finder.com
Qwilt (edge cloud provider)	edge.ds-c7114-microsoft.global.dns.qwilted-cds.cqloud.com
Sentry (app monitoring)	o4506026096263169.ingest.sentry.io
Tealium CDN	tags.tiqcdn.com
Usabilla (verzamelt feedback op websites)	w.usabilla.com
VWO (analytics)	dev.visualwebsiteoptimizer.com

3.1.1.29 Overzicht met en zonder Netskope

Tabel 2: Lang overzicht van alle domeinen en wijze van waarneming (tot p. 33)

Host	Netskope Wireshark	Zonder Netskope Wireshark	Zonder Netskope Mitmproxy
da-pr-ecslo-16vz8llff1sru-159561671.eu-central-1.elb.amazonaws.		✓	
wxt-registration-ingressgateway.acmhwxt-prd-1.prod.infra.webex.		✓	
wxt-registration-ingressgateway.acmhwxt-prd-4.prod.infra.webex.		✓	
wxt-registration-ingressgateway.afrawxt-prd-1.prod.infra.webex.		✓	
wxt-registration-ingressgateway.afrawxt-prd-2.prod.infra.webex.		✓	
epx-enterpriseproxy-2.d03-046.ic3-calling-enterpriseproxy.01-we		✓	
[redacted]	✓		
[redacted]	✓		
[redacted]	✓		
[redacted]	✓		
[redacted]		✓	
[redacted]		✓	
[redacted]		✓	
[redacted]		✓	
[redacted]	✓		
[redacted]	✓		
[redacted]		✓	
[redacted]		✓	
[redacted]	✓		
[redacted]		✓	
[redacted]		✓	
[redacted]	✓		
[redacted]	✓		
[redacted]	✓		

5.1.2.h	✓	
		✓
	✓	
		✓
		✓
	✓	
		✓
	✓	
	✓	
		✓
		✓
		✓
		✓
		✓
		✓
		✓
	✓	
		✓
		✓
		✓
		✓
	✓	
	✓	
	✓	
		✓
		✓
		✓
	✓	
	✓	
		✓
	✓	
		✓
		✓

Docnr1

5.1.2.h		✓	
			✓
			✓
		✓	
		✓	
			✓
			✓
			✓
			✓
			✓
		✓	
			✓
			✓
			✓
		✓	
			✓
		✓	
			✓
		✓	
		✓	
			✓
prod-eu-resolver.naturallanguageeditorservice.osi.office.net.ak			✓
g2a02-26f0-1180-0035-0000-0000-0210-6ac5.deploy.static.akamaite			✓
sp-20191001060653164200000004-710657394.eu-west-1.elb.amazonaws			✓
api.ipdata.co			✓
ads-dpgmediabe.adhese.com			✓ ✓
user-sync.adhese.com			✓
acdn.adnxs.com			✓ ✓
ams3-ib.adnxs.com			✓
cdn.adnxs.com			✓ ✓
ib.adnxs.com			✓ ✓
media.adrcdn.com			✓ ✓
a23-38-23-24.deploy.static.akamaitechnologies.com			✓

a23-48-125-217.deploy.static.akamaitechnologies.com	✓		
a23-73-0-190.deploy.static.akamaitechnologies.com		✓	
a95-101-136-223.deploy.static.akamaitechnologies.com		✓	
s3-3-w.amazonaws.com		✓	
qnl-play-fetch.s3.amazonaws.com		✓	✓
cdn.amplitude.com		✓	
api.eu.amplitude.com		✓	
api-sr.eu.amplitude.com		✓	
api.lab.eu.amplitude.com		✓	✓
sr-client-cfg.eu.amplitude.com		✓	
ac99c40bc9e28338c.awsglobalaccelerator.com		✓	
iris-de-prod-azsc-v2-frc-b.francecentral.cloudapp.azure.com		✓	
onedscolprdfrc00.francecentral.cloudapp.azure.com		✓	
onedscolprdfrc07.francecentral.cloudapp.azure.com		✓	
osiprod-frc-bronze-azsc-000.francecentral.cloudapp.azure.com		✓	
osiprod-frc-buff-azsc-000.francecentral.cloudapp.azure.com		✓	
onedscolprdgwc06.germanywestcentral.cloudapp.azure.com		✓	
waws-prod-fra-037-8717.germanywestcentral.cloudapp.azure.com		✓	
amsub0302sfring.northeurope.cloudapp.azure.com		✓	
iris-de-prod-azsc-v2-neu.northeurope.cloudapp.azure.com		✓	
iris-de-prod-azsc-v2-neu-b.northeurope.cloudapp.azure.com		✓	
md-prod-simcon-ip0.northeurope.cloudapp.azure.com		✓	
md-prod-simcon-ip1.northeurope.cloudapp.azure.com		✓	
md-prod-simcon-ip128.northeurope.cloudapp.azure.com		✓	
md-prod-simcon-ip129.northeurope.cloudapp.azure.com		✓	
nmoendpoint.northeurope.cloudapp.azure.com		✓	
onedscolprdneu00.northeurope.cloudapp.azure.com		✓	
onedscolprdneu01.northeurope.cloudapp.azure.com		✓	
onedscolprdneu03.northeurope.cloudapp.azure.com		✓	
onedscolprdneu04.northeurope.cloudapp.azure.com		✓	
onedscolprdneu05.northeurope.cloudapp.azure.com		✓	
onedscolprdneu06.northeurope.cloudapp.azure.com		✓	
onedscolprdneu10.northeurope.cloudapp.azure.com		✓	

Docnr1

onedscolprdneu11.northeurope.cloudapp.azure.com	✓	
onedscolprdneu12.northeurope.cloudapp.azure.com	✓	
onedscolprdneu13.northeurope.cloudapp.azure.com	✓	
onedscolprdneu14.northeurope.cloudapp.azure.com	✓	
osiprod-neu-bronze-azsc-000.northeurope.cloudapp.azure.com	✓	
osiprod-neu-flax-azsc-000.northeurope.cloudapp.azure.com	✓	
prod-agic-ne-8.northeurope.cloudapp.azure.com	✓	
settings-prod-neu-1.northeurope.cloudapp.azure.com	✓	
settings-prod-neu-2.northeurope.cloudapp.azure.com	✓	
pexsucpeu03.swedencentral.cloudapp.azure.com	✓	
osiprod-uks-bronze-azsc-000.uksouth.cloudapp.azure.com	✓	
augloop-prod-pa00.westeurope.cloudapp.azure.com	✓	
augloop-prod-pd02.westeurope.cloudapp.azure.com	✓	
augloop-prod-pd04.westeurope.cloudapp.azure.com	✓	
md-prod-simcon-ip1.westeurope.cloudapp.azure.com	✓	
onedscolprdweu01.westeurope.cloudapp.azure.com	✓	
onedscolprdweu02.westeurope.cloudapp.azure.com	✓	
onedscolprdweu05.westeurope.cloudapp.azure.com	✓	
onedscolprdweu06.westeurope.cloudapp.azure.com	✓	
onedscolprdweu07.westeurope.cloudapp.azure.com	✓	
onedscolprdweu09.westeurope.cloudapp.azure.com	✓	
onedscolprdweu11.westeurope.cloudapp.azure.com	✓	
onedscolprdweu13.westeurope.cloudapp.azure.com	✓	
onedscolprdweu15.westeurope.cloudapp.azure.com	✓	
osiprod-weu-bronze-azsc-000.westeurope.cloudapp.azure.com	✓	
osiprod-weu-buff-azsc-000.westeurope.cloudapp.azure.com	✓	
prod-agic-we-4.westeurope.cloudapp.azure.com	✓	
www.bing.com	✓	✓
cdn.brandmetrics.com	✓	
collector.brandmetrics.com	✓	✓
btloader.com	✓	
api.btloader.com	✓	
htlb.casalemedia.com	✓	✓

ssum-sec.casalemedia.com	✓	
www.cisco.com	✓	✓
ds.ciscospark.com	✓	
edge.ds-c7114-microsoft.global.dns.qwilted-cds.cqloud.com	✓	
bidder.criteo.com	✓	✓
gbc2.fr3.eu.criteo.com	✓	
gbc8.nl3.eu.criteo.com	✓	
ag.gbc.criteo.com	✓	✓
gem.gbc.criteo.com	✓	✓
gum.criteo.com	✓	✓
gum.nl3.vip.prod.criteo.com	✓	
in-ftd-65.nl3.vip.prod.criteo.com	✓	
ag.dns-finder.com	✓	
applets.ebxcdn.com	✓	
www.eicar.com	✓	✓
default.exp-tas.com	✓	✓
star-mini.c10r.facebook.com	✓	
www.facebook.com	✓	✓
kit.fontawesome.com	✓	✓
region1.google-analytics.com	✓	
adservice.google.com	✓	
clients2.google.com	✓	✓
ogads-pa.clients6.google.com	✓	
youtube-ui.l.google.com	✓	
ytimg.l.google.com	✓	
play.google.com	✓	✓
www.google.com	✓	
pagead2.googlesyndication.com	✓	
www.googletagmanager.com	✓	
clients2.googleusercontent.com	✓	✓
googlehosted.l.googleusercontent.com	✓	
5.1.2.h	✓	
5.1.2.h	✓	

fonts.gstatic.com	✓	
pacman-content-live.live.eks.hotjar.com	✓	
wsky-live.live.eks.hotjar.com	✓	
script.hotjar.com	✓	
static.hotjar.com	✓	✓
static-cdn.hotjar.com	✓	
ws.hotjar.com	✓	✓
js-sec.indexww.com	✓	
platform.linkedin.com	✓	✓
login.live.com	✓	✓
odc.officeapps.live.com	✓	✓
euc.pptsgs.officeapps.live.com	✓	✓
roaming-eu.officeapps.live.com	✓	✓
uks-azsc-config.officeapps.live.com	✓	
weu-azsc-config.officeapps.live.com	✓	
eu-mobile.events.data.microsoft.com	✓	✓
eu-office.events.data.microsoft.com	✓	✓
edge.microsoft.com	✓	✓
graph.microsoft.com	✓	✓
fd.api.iris.microsoft.com	✓	✓
msedge.b.tlu.dl.delivery.mp.microsoft.com	✓	✓
array501.prod.do.dsp.mp.microsoft.com	✓	
array508.prod.do.dsp.mp.microsoft.com	✓	
array510.prod.do.dsp.mp.microsoft.com	✓	
array512.prod.do.dsp.mp.microsoft.com	✓	
array518.prod.do.dsp.mp.microsoft.com	✓	✓
array616.prod.do.dsp.mp.microsoft.com	✓	
disc501.prod.do.dsp.mp.microsoft.com	✓	✓
geo.prod.do.dsp.mp.microsoft.com	✓	✓
kv501.prod.do.dsp.mp.microsoft.com	✓	✓
officeclient.microsoft.com	✓	✓
prod.rewardsplatform.microsoft.com	✓	✓
prod-4c1.rewardsplatform.microsoft.com	✓	

europe.smartscreen.microsoft.com	✓	✓
teams.microsoft.com	✓	✓
config.teams.microsoft.com	✓	✓
pub-ent-euno-10-t.trouter.teams.microsoft.com	✓	✓
pub-ent-plce-01-t.trouter.teams.microsoft.com	✓	✓
login.microsoftonline.com	✓	✓
metrics.mopinion.com	✓	
survey-cache.mopinion.com	✓	
survey-collect.mopinion.com	✓	
survey-deploy.mopinion.com	✓	
augloop.office.com	✓	✓
westeurope-pd02.augloop.office.com	✓	✓
api.diagnostics-eudb.office.com	✓	✓
entitlement.diagnostics-eudb.office.com	✓	✓
incidents.diagnostics-eudb.office.com	✓	✓
AMS-efz.ms-acdc.office.com	✓	
outlook.office.com	✓	✓
substrate.office.com	✓	✓
eop-g2.tm-4.office.com	✓	
outlook.office365.com	✓	✓
autodiscover-s.outlook.com	✓	✓
cdn-eu.readspeaker.com	✓	✓
sb.scorecardresearch.com	✓	
dwrt1.sharepoint.com	✓	✓
config.edge.skype.com	✓	✓
api.smartocto.com	✓	
ingestion.smartocto.com	✓	
tentacles.smartocto.com	✓	✓
tags.tiqcdn.com	✓	✓
urbanlaurel.com	✓	
w.usabilla.com	✓	
dev.visualwebsiteoptimizer.com	✓	
avatar-a.wbx2.com	✓	✓

board-a.wbx2.com	✓	✓
client-upgrade-a.wbx2.com	✓	✓
conv-a.wbx2.com	✓	✓
encryption-a.wbx2.com	✓	✓
feature-broadcast-b.wbx2.com	✓	✓
idbroker-guest-a.wbx2.com	✓	✓
idbroker-guest-k.wbx2.com	✓	✓
llm1-connection-k.wbx2.com	✓	✓
locus-b.wbx2.com	✓	✓
mercury-connection-partition1-a.wbx2.com	✓	✓
metrics-a.wbx2.com	✓	✓
proximity-a.wbx2.com	✓	✓
u2c-a.wbx2.com	✓	✓
wdm-a.wbx2.com	✓	✓
wdm-k.wbx2.com	✓	✓
www-service-a.wbx2.com	✓	✓
binaries.webex.com	✓	✓
global-nebulab-jfk02-dfw01.webex.com	✓	
global-utsa.webex.com	✓	
idbroker.webex.com	✓	✓
wxt-general-ingressgateway.acmhwxt-prd-1.prod.infra.webex.com	✓	
wxt-message-ingressgateway.acmhwxt-prd-1.prod.infra.webex.com	✓	
wxt-ci-ingressgateway.acmhwxt-prd-2.prod.infra.webex.com	✓	
wxt-general-ingressgateway.acmhwxt-prd-2.prod.infra.webex.com	✓	
wxt-mercury-ingressgateway.acmhwxt-prd-2.prod.infra.webex.com	✓	
wxt-wxid-ingressgateway.acmhwxt-prd-3.prod.infra.webex.com	✓	
wxt-ci-ingressgateway.afrawxt-prd-1.prod.infra.webex.com	✓	
wxt-mercury-ingressgateway.afrawxt-prd-1.prod.infra.webex.com	✓	
wxt-general-ingressgateway.afrawxt-prd-2.prod.infra.webex.com	✓	
wxt-meet-ingressgateway.apdxwxt-prd-2.prod.infra.webex.com	✓	
calliope-anycast.prod.infra.webex.com	✓	
xlm59.public.wamsm-a-0.prod.infra.webex.com	✓	
join-test.webex.com	✓	✓

pricing.webex.com	✓	✓
prod-achm-general.svc.webex.com	✓	✓
prod-afra-general.svc.webex.com	✓	✓
u2c.svc.webex.com	✓	✓
tsa.webex.com	✓	✓
tsa3.webex.com	✓	✓
web.webex.com	✓	✓
www.webex.com	✓	✓
avatar-prod-us-east-2.webexcontent.com	✓	✓
img.youtube.com	✓	✓
www.youtube.com	✓	✓
partition-cname-trouter-ic3-edf-trouter-service-trouter-1.d02-0	✓	
partition-cname-trouter-ic3-edf-trouter-service-trouter-2.d02-0	✓	
cloud.ccm19.de	✓	
ep1.adtrafficquality.google	✓	
ep2.adtrafficquality.google	✓	
dns.google	✓	
target.digitalaudience.io	✓	✓
content.hotjar.io	✓	✓
o4506026096263169.ingest.sentry.io	✓	
otelrules.svc.static.microsoft	✓	✓
nmodpgendpoint.2cnt.net	✓	✓
a-0019.standard.a-msedge.net	✓	
prod-global-autodetect.acompli.net	✓	✓
ad-delivery.net	✓	
www.tm.a.prd.aadg.akadns.net	✓	
www.tm.v4.a.prd.aadg.akadns.net	✓	
www.tm.f.prd.aadg.akadns.net	✓	
weu.pptsgs.live.com.akadns.net	✓	
prodeu.officeenrichment.osi.office.net.akadns.net	✓	
prodeu.shredder.osi.office.net.akadns.net	✓	
eudbipv4.clients.config.office.akadns.net	✓	
a1579.d.akamai.net	✓	

a1894.dscb.akamai.net	✓	
a937.dscb.akamai.net	✓	
a1221.dscd.akamai.net	✓	
a1813.dscd.akamai.net	✓	
a1817.dscd.akamai.net	✓	
a1864.dscd.akamai.net	✓	
a360.dscd.akamai.net	✓	
a390.dscd.akamai.net	✓	
a726.dscd.akamai.net	✓	
a1847.dscg2.akamai.net	✓	
a1961.g2.akamai.net	✓	
a1968.i6g1.akamai.net	✓	
a978.i6g1.akamai.net	✓	
e3913.cd.akamaiedge.net	✓	
e10370.d.akamaiedge.net	✓	
e119.dsca.akamaiedge.net	✓	
e2867.dsca.akamaiedge.net	✓	
e184071.dscb.akamaiedge.net	✓	
e26769.dscb.akamaiedge.net	✓	
e27429.dscb.akamaiedge.net	✓	
e28241.dscb.akamaiedge.net	✓	
e67691.dscb.akamaiedge.net	✓	
e69879.dscb.akamaiedge.net	✓	
e127270.dscd.akamaiedge.net	✓	
e77980.dscd.akamaiedge.net	✓	
e86303.dscx.akamaiedge.net	✓	
e12627.g.akamaiedge.net	✓	
e6603.g.akamaiedge.net	✓	
ax-0002.ax-dc-msedge.net	✓	
ax-0002.ax-msedge.net	✓	
edge-consumer-static.azureedge.net	✓	✓
edgeassetservice.azureedge.net	✓	✓
realtime-tentacles-production.b-cdn.net	✓	

bx-9999.bx-msedge.net	✓	
kit.fontawesome.com.cdn.cloudflare.net	✓	
cdn.jsdelivr.net.cdn.cloudflare.net	✓	
d162h6x3rxav67.cloudfront.net	✓	
d16t1nucl0wcte.cloudfront.net	✓	
d2f5rvg67fro0x.cloudfront.net	✓	
d2xvo51pr40ne7.cloudfront.net	✓	
d3l8kopw1d3uiv.cloudfront.net	✓	
d96vky0xjhjcq.cloudfront.net	✓	
dzfq4ouujrxm8.cloudfront.net	✓	
t.contentsquare.net	✓	
dnacdn.net	✓	
ad.doubleclick.net	✓	
cm.g.doubleclick.net	✓	✓
googleads.g.doubleclick.net	✓	
dmoi.api.dpgmedia.net	✓	✓
c.dpgmedia.net	✓	✓
myprivacy-static.dpgmedia.net	✓	✓
s-0005.dual-s-dc-msedge.net	✓	
s-0005.dual-s-msedge.net	✓	
e-0014.e-msedge.net	✓	
connect.facebook.net	✓	✓
amplitude.map.fastly.net	✓	
prod.appnexus.map.fastly.net	✓	
jsdelivr.map.fastly.net	✓	
linkedin.map.fastly.net	✓	
s-part2-t-9999.fb-t-msedge.net	✓	
s-part-0039.t-0009.fb-t-msedge.net	✓	
t-9999.fb-t-msedge.net	✓	
scontent.xx.fbcdn.net	✓	
cdn.jsdelivr.net	✓	✓
k-9999.k-msedge.net	✓	
l-0007.l-msedge.net	✓	

ln-9999.ln-msedge.net	✓	
static.edge.microsoftapp.net	✓	✓
mil30r9a.msedge.net	✓	
omex.cdn.office.net	✓	✓
res.cdn.office.net	✓	✓
statics.teams.cdn.office.net	✓	✓
binaries.templates.cdn.office.net	✓	✓
metadata.templates.cdn.office.net	✓	✓
support.content.office.net	✓	✓
exo.nel.measure.office.net	✓	✓
prodeu.enrichment.osi.office.net	✓	✓
nleditor.osi.office.net	✓	✓
shredder-eu.osi.office.net	✓	✓
s-0005.s-msedge.net	✓	
s-0006.s-msedge.net	✓	
ad.sxp.smartclip.net	✓	
dual-spo-0005.spo-msedge.net	✓	
s-part-0039.t-0009.t-msedge.net	✓	
www.tm.a.prd.aadg.trafficmanager.net	✓	
www.tm.prd.ags.trafficmanager.net	✓	
beta-autodetect.outlookmobile.com.trafficmanager.net	✓	
global-entry-sts.trafficmanager.net	✓	
wac-9999.wac-msedge.net	✓	
web.blz22prdstr01a.store.core.windows.net	✓	
officewhatsnew.z13.web.core.windows.net	✓	✓
login.dpgmedia.nl	✓	✓
www.google.nl	✓	
minbzk.nl	✓	
end.nmo-ep.nl	✓	✓
images.nu.nl	✓	✓
login.nu.nl	✓	✓
pg.nu.nl	✓	✓
www.nu.nl	✓	✓

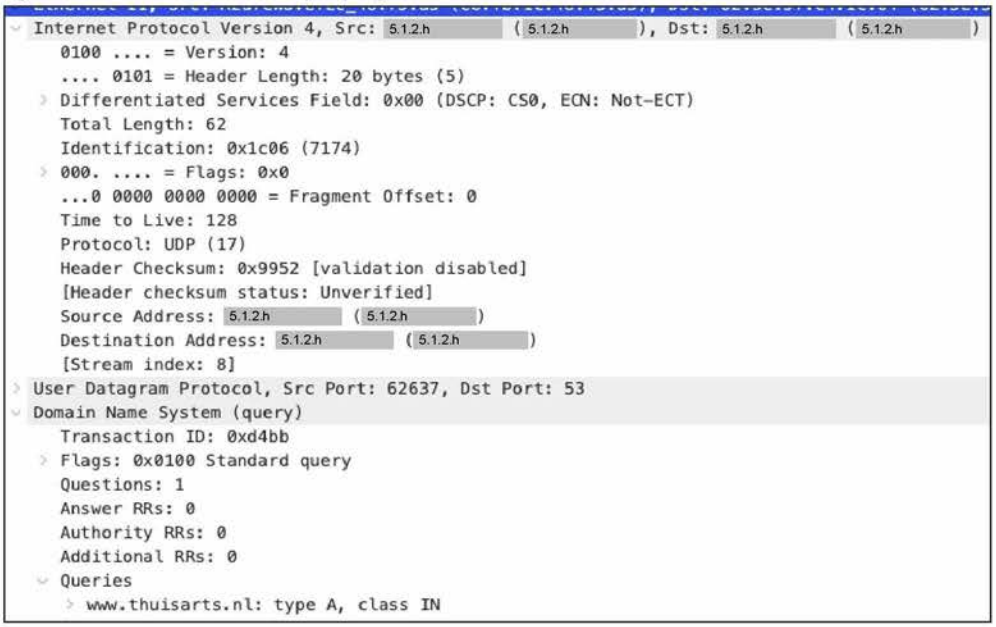
widgets.pexi.nl	✓	✓
5.1.2.h	✓	✓
	✓	✓
	✓	✓
	✓	✓
5.1.2.h	✓	✓
www.rijksoverheid.nl	✓	
5.1.2.h	✓	
stats.thuisarts.nl	✓	
www.thuisarts.nl	✓	
ade.weborama.nl	✓	
mrq.weborama.nl	✓	
5.1.2.h	✓	
5.1.2.h	✓	
cdn.cookielaw.org	✓	
eicar.org	✓	✓
secure.eicar.org	✓	
www.eicar.org	✓	✓
5.1.2.h	✓	

3.1.2 Geobserveerde protocollen

3.1.2.1 DNS (poort 53)

Tijdens het testen is alleen DNS-verkeer geobserveerd naar een DNS resolver op het lokale netwerk. Op een vertrouwd netwerk vormt dit verkeer geen ongebruikelijk risico. Maar op onvertrouwde netwerken, bij medewerkers thuis, of onderweg in hotels of cafés, kan dat betekenen dat de domeinnamen waarmee de medewerker verbinding maakt uitlekken.

Figuur 1: Voorbeeld van DNS query bij bezoek aan thuisarts.nl



3.1.2.2 HTTP (poort 80)

Vrijwel al het web-verkeer gaat tegenwoordig over een versleutelde verbinding (HTTPS). Toch zijn er tijdens het testen niet-versleutelde HTTP verbindingen opgemerkt die het lokale netwerk verlieten.

Het verkeer naar Akamai heeft waarschijnlijk te maken met een check of het TLS/SSL certificaat van de website is ingetrokken (TLS/SSL *certificate revocation*). Dat is dus een essentiële en onvermijdelijke beveiligingscheck.

Het IP-adres 5.1.2.h is van Fastly (CDN). De inhoud van dit verkeer is beperkt tot het maken en sluiten van een verbinding, zonder inhoud te versturen.

Het eerste van de twee Microsoft-adressen, eindigend op cqloud.com, wordt benaderd door de BITS-client (*Background Intelligent Transfer Services*), een onderdeel van Windows dat software updates binnenhaalt.

Het tweede aangetroffen Microsoft-adres, dat eindigt op mp.microsoft.com, heeft te maken met auto update functionaliteit van de browser Edge.

Tabel 4: Verzonden en ontvangen bytes per host poort 80

Host	HTTP reqs	Verzonden Bytes	Ontvangen Bytes
5.1.2.h	0	108	108
edge.ds-c7114-microsoft.global.dns.qwilted-cds.cqloud.com	0	693	931
msedge.b.tlu.dl.delivery.mp.microsoft.com	14	0	0

a1961.g2.akamai.net	0	393	415
a1968.i6g1.akamai.net	0	86	0
a978.i6g1.akamai.net	0	344	0
e3913.cd.akamaiedge.net	0	570	1100

3.1.2.3 Windows Fileshare (poort 445)

Tijdens het testen is een kleine hoeveelheid Windows Fileshare (SMB) verkeer geobserveerd naar drie IP-adressen die bestemd zijn voor *carrier-grade NAT*. Vanwege de aard van de IP-range kan Privacy Company niet vaststellen aan wie deze IP-adressen zijn toegewezen. De verbindingspogingen vanuit de onderzoekslaptops resulteerden niet in een antwoord. Daardoor was het niet mogelijk om vast te stellen of de IP-adressen in gebruik waren op het moment van testen. Het betreft o.a. pogingen om bestanden te openen (zoals '5.1.2.h _" of 5.1.2.h) of om een sessie te beëindigen. Privacy Company kan niet inschatten wat de oorzaak van deze verbindingen is en wat het risico is als deze berichten worden ontvangen door een derde partij.

Tabel 5: Verzonden en ontvangen bytes per host poort 445

Host	Verzonden Bytes	Ontvangen Bytes
5.1.2.h	438	0
	504	0
	1398	0

3.1.2.4 Windows Update Delivery Optimization WUDO (poort 7680)

Wanneer Windows zoekt naar Windows-updates en downloads uit de Microsoft Store, probeert Windows eerst op het lokale netwerk andere computers te vinden die deze bestanden al hebben. Microsoft laat de lokale systemen dus de toegang tot de updates delen. Microsoft gebruikt deze methode om netwerkcapaciteit te besparen voor zowel de klanten als voor Microsoft. In het waargenomen verkeer zijn verbindingen te zien met *carrier-grate NAT* (100.*.*.*) naar een ongebruikte lokale netwerkadresruimte (172.*.*.*) en naar een enkel adres dat eigendom is van Mercedes Benz, zoals aangegeven in Figuur 2 hieronder.

Figuur 2: Relevant onderdeel WHOIS resultaat Mercedes Benz

i net num 5.1.2.h

netname:	MERCEDES-BENZ-NET1
org:	ORG-DA474-RIPE
descr:	Mercedes-Benz Group AG
country:	DE
admin-c:	EH4384-RIPE
tech-c:	EH4384-RIPE
status:	LEGACY
mnt-by:	RIPE-NCC-LEGACY-MNT
mnt-by:	DAIMLER-MNT
created:	1970-01-01T00:00:00Z
last-modified:	2022-04-12T08:04:16Z
source:	RIPE

Privacy Company heeft alleen een aantal TCP SYN pakketten geobserveerd en vier pogingen per SYN pakket om het pakket opnieuw te versturen, maar nul ontvangen bytes. Dat betekent dat er geen inhoudelijk verkeer is verstuurd en er alleen pogingen zijn gedaan om verbinding te maken.

SSC-ICT heeft met een schermafbeelding aangetoond dat Netskope het verkeer naar dit IP-adres al standaard blokkeerde. Dit is kennelijk by default verhindert door Netskope, maar Privacy Company adviseert SSC-ICT om al het verkeer naar Windows Update poort 7680 te blokkeren.

Tabel 6: Verzonden en ontvangen bytes Windows Update Delivery Optimization

Host	Verzonden Bytes	Ontvangen Bytes
5.1.2.h	330	0
	264	0
	330	0
	330	0
	132	0
	330	0
	330	0
	330	0
	330	0
	330	0
	330	0
	330	0
	330	0

5.1.2.h	330	0
	330	0
	66	0
	330	0
	330	0
	330	0
	330	0
	330	0
	330	0
	330	0
	330	0
	330	0
	330	0
	330	0
	330	0
	330	0
	330	0

3.1.3 Geobserveerde cookies

Tabel 7: Hosts en waargenomen verschillende cookies per host

Host	Cookies
acdn.adnxs.com	uuid2 XANDR_PANID icu
cdn.adnxs.com	uuid2 XANDR_PANID icu
ib.adnxs.com	uuid2 icu XANDR_PANID

www.bing.com	SRCHUID SRCHD _EDGE_V MUID SRCHUSR SRCHHPGUSR MUIDB _EDGE_S, _SS
htlb.casalemedia.com	receive-cookie-deprecation
www.cisco.com	c_bi
gum.criteo.com	uid
odc.officeapps.live.com	MUID
euc.pptsgs.officeapps.live.com	MUID
prod.rewardsplatform.microsoft.com	MC1 kndctr_EA76ADE95776D2EC7F000101_AdobeOrg_identity AMCV_EA76ADE95776D2EC7F000101%40AdobeOrg
login.microsoftonline.com	buid fpc esctx x-ms-gateway-slice stsservicecookie
idbroker.webex.com	JSESSIONID amlbcookie amlbcookiesm wxidIstio
join-test.webex.com	origin_web _fbp OptanonAlertBoxClosed bm_mi bm_sv OptanonConsent ak_bmsc utag_main WBX_kubed_j2eeapp JSESSIONID CK_M_ACLK _csrf_ trackingSessionID
pricing.webex.com	origin_web _fbp OptanonAlertBoxClosed bm_mi bm_sv OptanonConsent ak_bmsc utag_main machineId webexInstallSuccess
web.webex.com	origin_web _fbp OptanonAlertBoxClosed bm_mi bm_sv

	OptanonConsent ak_bmsc utag_main machineId
www.webex.com	origin_web head_locale user_locale user_lang user_currency _fbp OptanonAlertBoxClosed OptanonConsent utag_main affinity ak_bmsc bm_mi
img.youtube.com	__Secure-ROLLOUT_TOKEN VISITOR_INFO1_LIVE VISITOR_PRIVACY_METADATA
www.youtube.com	__Secure-ROLLOUT_TOKEN VISITOR_INFO1_LIVE VISITOR_PRIVACY_METADATA YSC
target.digitalaudience.io	digitalAudience
cm.g.doubleclick.net	ar_debug receive-cookie-deprecation IDE
myprivacy-static.dpgmedia.net	sp
login.dpgmedia.nl	_abck ak_bmsc bm_sz
images.nu.nl	authId CookieConsent dpg-consent-string _vwo_uuid_v2 tcf20_purposes _pcid cX_P _fbp cX_G _pctx _pubcid _pubcid_cst _ 5.1.2.h _awl _sp_id.dcc9 cto_bundle cto_bidid cto_dna_bundle
login.nu.nl	authId CookieConsent dpg-consent-string _vwo_uuid_v2 tcf20_purposes _pcid cX_P

	_fbp cX_G _abck ak_bmsc bm_sz _pctx _pubcid _pubcid_cst 5.1.2.h _awl _sp_id.dcc9 cto_bundle cto_bidid cto_dna_bundle bm_sv
pg.nu.nl	authId CookieConsent dpg-consent-string _vwo_uuid_v2 tcf20_purposes _pcid cX_P _fbp cX_G ak_bmsc _pctx _pubcid _pubcid_cst 5.1.2.h _awl _sp_id.dcc9 cto_bundle cto_bidid cto_dna_bundle bm_sv
www.nu.nl	authId CookieConsent dpg-consent-string _vwo_uuid_v2 tcf20_purposes _pcid cX_P _fbp cX_G last_visit_timestamp ak_bmsc NU-cx_done _pctx _pubcid _pubcid_cst 5.1.2.h _awl _sp_id.dcc9 _sotmpid cto_bundle cto_bidid cto_dna_bundle bm_sv
eicar.org	__wpdm_client, PHPSESSID
www.eicar.org	__wpdm_client, PHPSESSID

3.1.4 Telemetrieberichten

Een typisch Windows-telemetriebericht bevat een uniek nummer, een tijdstempel, verschillende unieke identificatiegegevens voor de eindgebruiker en het apparaat, en verschillende stukjes informatie over bijvoorbeeld het type apparaat, de schermgrootte, het besturingssysteem, de software en/of het stuurprogramma. Het gaat om éénrichtingsverkeer naar Microsoft, zonder dat er een antwoord terugkomt. Het is dus een extra datastroom vanuit het apparaat van de eindgebruiker, los van de functionele verkeersuitwisseling om via internet met de Microsoft clouddiensten te praten.

Privacy Company heeft de telemetriestroom op twee manieren bekeken: met de Diagnostic Data Viewer app op Windows, en in het netwerkverkeer.

De waargenomen telemetrie datastroom vanuit Windows is beperkt tot noodzakelijke telemetrieberichten uit Windows om de diensten goed-werkend, veilig en up-to-date te houden. SSC-ICT heeft niet de aanbeveling opgevolgd om het telemetrieniveau op 'security' in te stellen (gelijk aan 'uit' zetten), maar heeft gekozen voor het niveau '*Required*'. Microsoft waarschuwt systeembeheerders nadrukkelijk dat het uitzetten van de telemetrie ertoe kan leiden dat de Windows update functionaliteit niet goed meer werkt.

Figuur 3: Waarschuwing Microsoft om Windows telemetrie niet uit te zetten[3]

> ⓘ **Note**
>
> If your organization relies on Windows Update, the minimum recommended setting is **Required diagnostic data**. Because no Windows Update information is collected when diagnostic data is off, important information about update failures isn't sent. Microsoft uses this information to fix the causes of those failures and improve the quality of our updates.

De aangetroffen berichten bevatten géén inhoudelijke gegevens die medewerkers hebben verwerkt op Windows (met Office 365) in de vorm van bijvoorbeeld inhoud of namen van mails, chats of bestanden, met uitzondering van de namen van externe apps of drivers. Privacy Company heeft geen specifieke Edge-telemetrie gezien. Op Windows 11 biedt Microsoft verschillende controles aan voor de Windows telemetrie en voor de Edge telemetrie. Net als op Windows is het mogelijk om de telemetrie uit de Edge browser helemaal uit te zetten, hoewel Microsoft dat niet aanbeveelt.[4] Microsoft noemt geen bezwaren tegen het uitzetten. Uit het ontbreken van Edge telemetrieberichten leidt Privacy Company af dat SCC-ICT de Edge telemetrie heeft uitgezet.

---

[3] Microsoft, Diagnostic data off, laatste update 29 juli 2025, URL: https://learn.microsoft.com/en-us/windows/privacy/configure-windows-diagnostic-data-in-your-organization#diagnostic-data-off (pagina laatst bezocht 8 augustus 2025).

[4] Microsoft, DiagnosticData (in Edge, toevoeging Privacy Company), laatste update 9 mei 2025, URL: https://learn.microsoft.com/en-us/deployedge/microsoft-edge-browser-policies/diagnosticdata#description (pagina laatst bezocht 8 augustus 2025).

De telemetrieberichten over de Windows Store gaan over het updaten van interne Windows componenten zoals de Windows camera, Windows To Do, Paint, Notepad, Screensketch, iets onduidelijks met Crossdevice, de Desktop app installer en Windows alarms, maar gaat ook over het updaten van externe drivers (bijvoorbeeld voor de HP Audio Control), en externe apps zoals de Display link manager en HP system information. Zie het voorbeeld van de volledige inhoud van 1 telemetriebericht hieronder, zie Figuur 4 hieronder. Om deze gegevensstroom te voorkomen, zou SSC-ICT moeten onderzoeken of het mogelijk is om de telemetrie uit te zetten zonder essentiële functionaliteit te verliezen.

Privacy Company heeft geen onderzoek gedaan naar uitgaande telemetrie en Required Service Data van Office 365.

Het eerste bericht in Tabel 7 hieronder bevat informatie over de updates van de browser Edge (met de naam 5.1.2.h). Deze berichten bevatten geen inhoud, maar wel veel velden die zeer gedetailleerde configuratie variabelen onthullen.

Microsoft bewaart sommige telemetrieberichten uit Windows 28 dagen, andere berichten langer, zonder specificatie hoe lang dat is, anders dan de mededeling *"particularly when the information is used to keep the device secure, up to date, and working as expected."*[5]

Privacy Company heeft geanalyseerd hoeveel van de aangetroffen telemetrieberichten door Microsoft heeft gedocumenteerd (op het ingestelde *Required* niveau).[6] Als dat zo is, staat er een groen vinkje in de derde kolom van Tabel 7 hieronder, met een hyperlink naar de documentatie. Er ontbreekt documentatie over 15 van de 39 aangetroffen soorten telemetrieberichten. Over de inhoud van de Required Diagnostic Data schrijft Microsoft dat ze onder andere de namen van apps en drivers verzamelt, zoals ook aangetroffen tijdens het onderzoek.

"Required diagnostic data is minimum data necessary to help keep the Windows operating system and integrated apps and services secure, up to date and performing as expected. Examples include information about the version of the operating system, apps and drivers installed on the device, whether updates were successfully installed, and details about your device and its settings that could impact keeping the device secure, up to date, and performing as expected."[7]

[5] Microsoft, Configure Windows diagnostic data in your organization, laatste update van 29 juli 2025, URL: https://learn.microsoft.com/en-us/windows/privacy/configure-windows-diagnostic-data-in-your-organization.

[6] Microsoft, Required diagnostic events and fields for Windows 11, version 24H2, URL: https://learn.microsoft.com/en-us/windows/privacy/required-diagnostic-events-fields-windows-11-24h2

[7] Microsoft, Data collection summary for Windows, April 2025, URL: https://www.microsoft.com/en-us/privacy/data-collection-windows (pagina laatst bezocht op 8 augustus 2025).

Tabel 8: Aangetroffen telemetrieberichten, aantal en naam

Naam van het telemetriebericht	Aantal	Microsoft documentatie
5.1.2.h	5	√
5.1.2.h	2	√
Microsoft.OSG.DU.DeliveryOptClient.DownloadCompleted	78	√
Microsoft.OSG.DU.DeliveryOptClient.DownloadStarted	78	√
Microsoft.Windows.Defender.Shield.HardwareSecurityFeatures	5	
Microsoft.Windows.DriverInstall.DeviceInstall	1	
Microsoft.Windows.FeatureQuality.Heartbeat	2	√
Microsoft.Windows.Inventory.Core.AmiTelCacheChecksum	1	
Microsoft.Windows.Inventory.Core.InventoryDevicePnpAdd	6	
Microsoft.Windows.Kernel.DeviceConfig.DeviceConfig	7	
Microsoft.Windows.OneSettingsClient.Heartbeat	2	√
Microsoft.Windows.OneSettingsClient.OneSettingsPayloadDownload2	8	
Microsoft.Windows.Security.CodeIntegrity.Wintrust.AggregatedCertificateCount	1	
Microsoft.Windows.Security.CodeIntegrity.Wintrust.AggregatedEncodedCertificates	4	
Microsoft.Windows.Security.CodeIntegrity.Wintrust.AggregatedSignatureCount	3	
Microsoft.Windows.Security.CodeIntegrity.Wintrust.AggregatedSignatureEvents	11	
Microsoft.Windows.Security.KeyGuard.KeyguardAdoption	34	
Microsoft.Windows.StoreAgent.Telemetry.BeginAcquireLicense	4	√
Microsoft.Windows.StoreAgent.Telemetry.BeginDownload	4	√
Microsoft.Windows.StoreAgent.Telemetry.BeginInstall	4	√
Microsoft.Windows.StoreAgent.Telemetry.BlockLowPriorityWorkItems	1	√
Microsoft.Windows.StoreAgent.Telemetry.DiagError	1	
Microsoft.Windows.StoreAgent.Telemetry.EndAcquireLicense	4	√
Microsoft.Windows.StoreAgent.Telemetry.EndDownload	4	√
Microsoft.Windows.StoreAgent.Telemetry.EndInstall	4	√
Microsoft.Windows.StoreAgent.Telemetry.EndScanForUpdates	2	√
Microsoft.Windows.StoreAgent.Telemetry.FulfillmentComplete	4	√

Microsoft.Windows.StoreAgent.Telemetry.FulfillmentInitiate	4	√
Microsoft.Windows.StoreAgent.Telemetry.ResumeInstallation	1	√
Microsoft.Windows.StoreAgent.Telemetry.ScheduleWorkWithUO	1	√
Microsoft.Windows.StoreAgent.Telemetry.StateTransition	10	√
Microsoft.Windows.StoreAgent.Telemetry.UnblockLowPriorityWorkItems	1	√
Microsoft.Windows.Update.Orchestrator.UpdatePolicyCacheRefresh	1	√
Microsoft.Windows.Update.WUClient.CheckForUpdatesSucceeded	2	√
Microsoft.Windows.Update.WUClient.DownloadSucceeded	8	[8]
Microsoft.Windows.Update.WUClient.InstallStarted	4	√
Microsoft.Windows.Update.WUClient.InstallSucceeded	4	√
Microsoft.Windows.UpdateReserveManager.InitializeReserves	2	
Microsoft.Windows.UpdateReserveManager.InitializeUpdateReserveManager	8	

Figuur 4: Inhoud van 1 telemetriebericht over het updaten van de (externe) DisplayLink.DisplayLinkManager


```
{
   "ver": "4.0",
   "name": "Microsoft.Windows.StoreAgent.Telemetry.BeginDownload",
   "time": "2025-05-22T11:56:32.5470996Z",
   "iKey": "5.1.2.h                                    ",
   "ext": {
      "utc": {
         "aId": "D5DD5CA4-33B8-40EA-A565-D7726F74207B",
         "eventFlags": 258,
         "pgName": "WINCORE",
         "dvcSample": 29.22,
         "flags": 52448199172,
         "edition": 4,
         "epoch": "502486",
         "seq": 592
      },
      "privacy": {
         "dataType": 2147483648,
         "isRequired": true,
         "dataCategory": 1,
         "product": 1
      },
      "metadata": {
         "privTags": 2147483648,
         "policies": 0
      },
      "mscv": {
         "cV": "rnmzafOyMUCLoPUi.1.2"
      },
      "os": {
         "bootId": 4,
```


[8] Microsoft documenteert wel andere telemetrieberichten over installatie van de WUClient.

```
        "name": "Windows",
        "ver": "10.0.26100.4061.amd64fre.ge_release.240331-1435",
                                                                                                    "expId":
"RS:26DF5,MD:283BAEF,ME:3038CEC,ME:3039059,ME:33B9AFF,ME:33B9B11,ME:33B9B19,MD:33B9B24,ME:3536BD9,MD
:2FE0A31,MD:2FE0A40,MD:2FE0A4F"
      },
      "app": {
                                                                                                    "id":
"W:0000f519feec486de87ed73cb92d3cac802400000000!000055efb424933087d755b18468bc574db4463d9ce6!svchost.exe",
        "ver": "2104/11/12:20:36:41!19466!svchost.exe",
        "is1P": 1,
        "asId": 452
      },
      "device": {
        "localId": "5.1.2.h                                                    ",
        "deviceClass": "Windows.Desktop"
      },
      "protocol": {
        "devMake": "HP",
        "devModel": "HP EliteBook 855 G8 Notebook PC",
        "ticketKeys": [
          "16783377"
        ]
      },
      "user": {
        "localId": "o:3"
      },
      "loc": {
        "tz": "+02:00"
      }
    },
    "data": {
      "ProductId": "9N09F8V8FS02",
      "PFN": "DisplayLink.DisplayLinkManager_3hxb1yeew1fh8",
      "CategoryId": "83b713a2-2657-4007-8256-1a63c34d8885",
      "BundleId": "",
      "IsUpdate": 1,
      "IsRemediation": 0,
      "IsInteractive": 0,
      "IsMandatory": 1,
      "IsRestore": 0,
      "AttemptNumber": 1,
      "SystemAttemptNumber": 1,
      "UserAttemptNumber": 0,
      "ClientAppId": "Update;ScanForUpdates-taskhostw-SearchForAllUpdatesWithUpdateOptionsAsync",
      "ParentBundleId": "",
      "IsBundle": 0,
      "WUContentId": "7fa1e50d-b648-9ad4-c543-041de0719425",
      "AggregatedPackageFullNames": "DisplayLink.DisplayLinkManager_3.2.14.0_neutral_~_3hxb1yeew1fh8"
    }
}
```


3.2 macOS (met en zonder Netskope)

Net als in het voorgaande deel is deze analyse van het uitgaand verkeer op DWR 2.0 op een Macbook onderverdeeld in een aantal paragrafen. Anders dan Microsoft, biedt Apple geen aparte tool aan om de uitgaande telemetrieberichten waar te nemen. Daarom is er geen vierde paragraaf met analyse van de telemetrieberichten.

Paragraaf 3.2.1 bevat een tabel met alle eindpunten die op MacOS zijn waargenomen naar de (vermoedelijke) gebruiker. De resultaten zijn grotendeels vergelijkbaar met de resultaten op Windows, met een paar andere domeinen. Het websitebezoek was verantwoordelijk voor het merendeel van het waargenomen verkeer, inclusief verkeer naar advertentienetwerken, grote webhosting partijen zoals AWS en Content Delivery Networks van Akamai en Cloudflare.

Het meeste verkeer is onderschept zonder Netskope, omdat Netskope een tunnel vormt tussen de laptop van de medewerker en de Netskope servers die SCC-ICT lokaal beheert. Het meeste verkeer lijkt daarom alleen naar de Netskope server te gaan. Alleen onversleuteld verkeer kon worden bekeken, zoals verkeer vanuit poort 80. Daarom lijkt het alsof Netskope nauwelijks verkeer doorlaat naar externe partijen in Tabel 8. Maar dat is niet de juiste conclusie: Netskope maakte alleen het onderscheppen van versleuteld verkeer onmogelijk, maar Netskope is niet bedoeld om tracking verkeer tegen te houden.

In paragraaf 3.2.2 is het waargenomen netwerkverkeer uitgesplitst naar protocol, zoals DNS-verkeer, HTTP of specifiek MacOS verkeer.

Paragraaf 3.2.3 bevat een tabel met de waargenomen cookies. Die bevat vooral advertentie en tracking analytics cookies die door de bezochte websites zijn geplaatst, met een paar uitzonderingen van cookies die door gebruik van de functionele applicaties zijn geplaatst.

3.2.1 Geobserveerde netwerk eindpunten

In onderstaande tabel is het verkeer naar Apple gehighlight in groen. Het verkeer naar Microsoft is gehighlight in geel, terwijl het verkeer naar Cisco Webex is gehighlight in blauw. Het verkeer naar Cisco is vergelijkbaar op beide besturingssystemen.

Het verkeer naar Apple bevat 9 eindpunten:

1. token.safebrowsing.apple
2. app-site-association.g.aaplimg.com (geen leesbare inhoud)
3. safebrowsing.g.aaplimg.com (geen leesbare inhoud)
4. cdn.smoot.g.aaplimg.com (geen leesbare inhoud)
5. smoot-searchv2-aeun1b.v.aaplimg.com (geen leesbare inhoud)
6. api-glb-aeun1b.smoot.apple.com
7. cdn2.smoot.apple.com
8. stocks-data-service.apple.com (beurskoerzen widget)
9. weatherkit.apple.com (weer widget)

De eerste domeinnaam (token.safebrowsing.apple) wijst op het gebruik van Google Safebrowsing door Apple. Apple noemt dit 'Fraudulent Website Warning' en legt uit dat Safari een soort hash naar Google

Safe Browsing en naar zichzelf stuurt, om te controleren of de website frauduleus is of malware bevat. Apple schrijft ook: *"The actual website address is never shared with the safe browsing provider."* [9]

Apple legt uit dat Google het IP-adres logt van de werknemer: *"Google (...) may also log your IP address when information is sent to them."*[10]
SSC-ICT kan dat voorkomen door Fraudulent Website Warnings uit te zetten en te kiezen voor een andere bescherming. Apple schrijft: *"You can disable Fraudulent Website Warnings in Safari at any time by going to Settings > Apps > Safari and tapping to turn off Fraudulent Website Warning."*[11]

Het zesde domein (api-glb-aeun1b.smoot.apple.com) ontvangt inhoudelijke gegevens over zoekopdrachten met Spotlight. Dat is een zoekfunctie die lokaal bestanden doorzoekt, maar ook websuggesties verzamelt, en daarom de zoekopdracht naar Apple stuurt. Figuur 5 bevat de inhoud van de zoekopdracht naar 'Covid'.

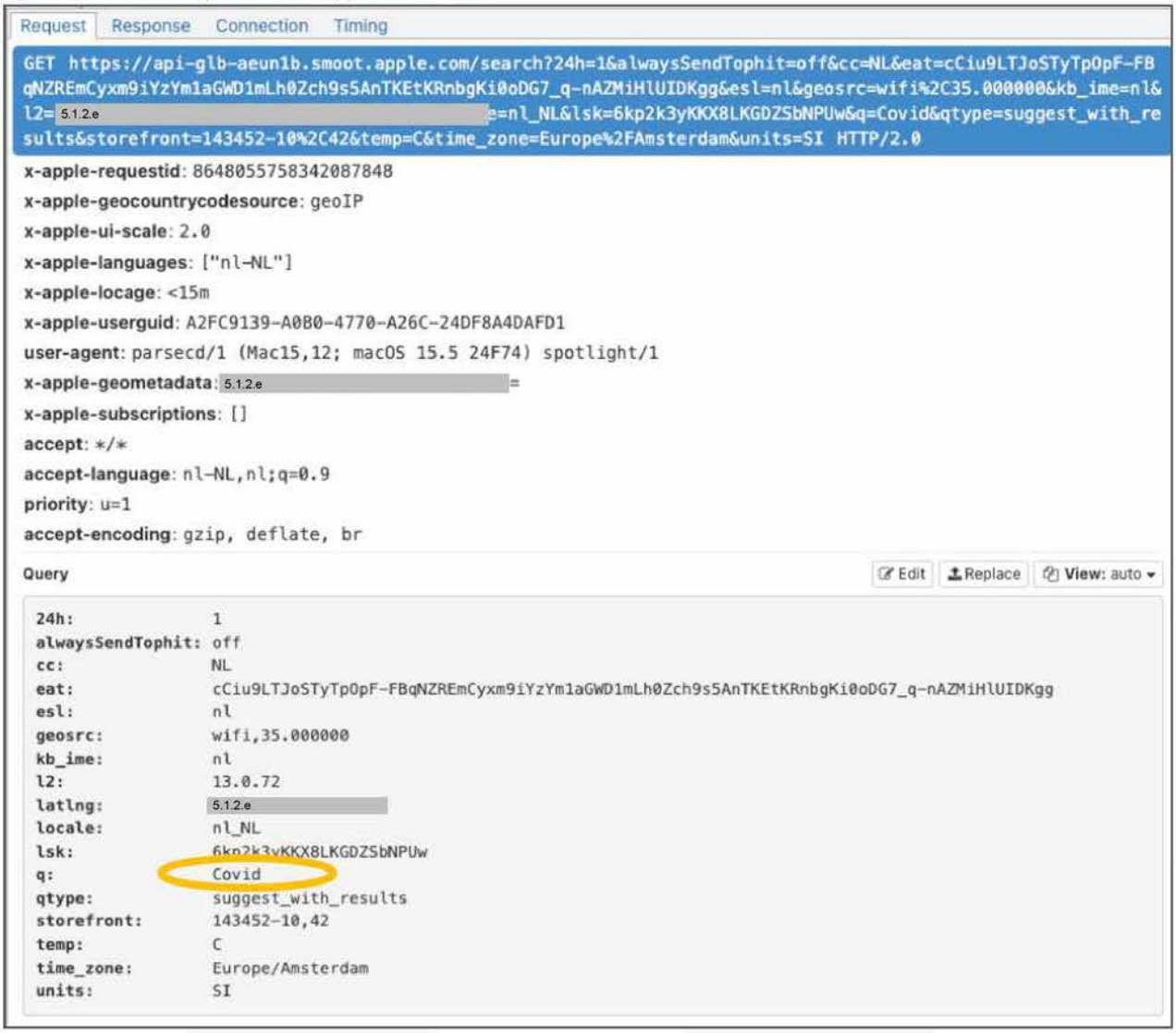
[9] Apple, Safari & Privacy, URL: https://www.apple.com/legal/privacy/data/en/safari/.

[10] Idem.

[11] Ibid.

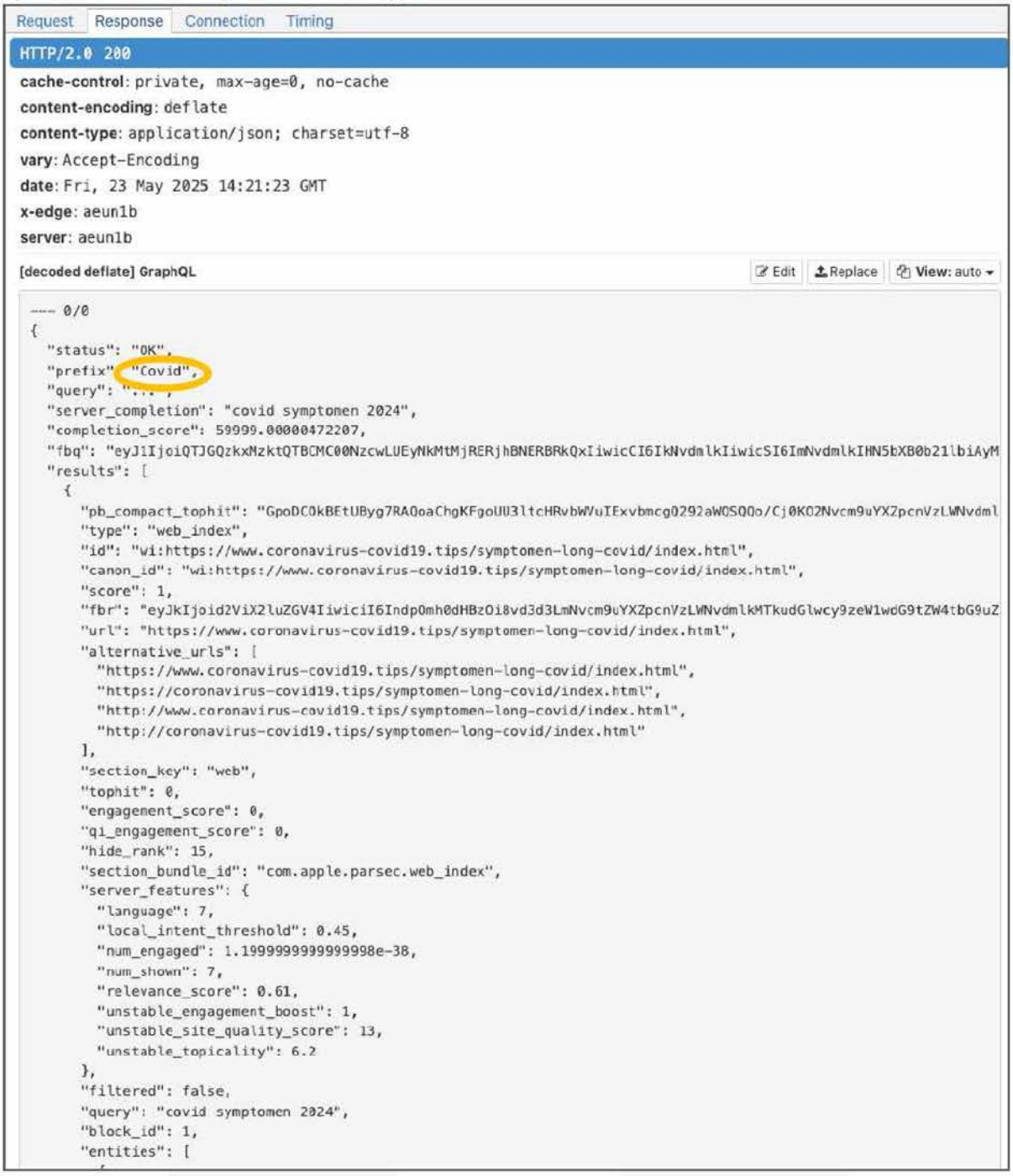
Docnr1

Figuur 5: Verzonden opdracht aan Apple over 'Covid'



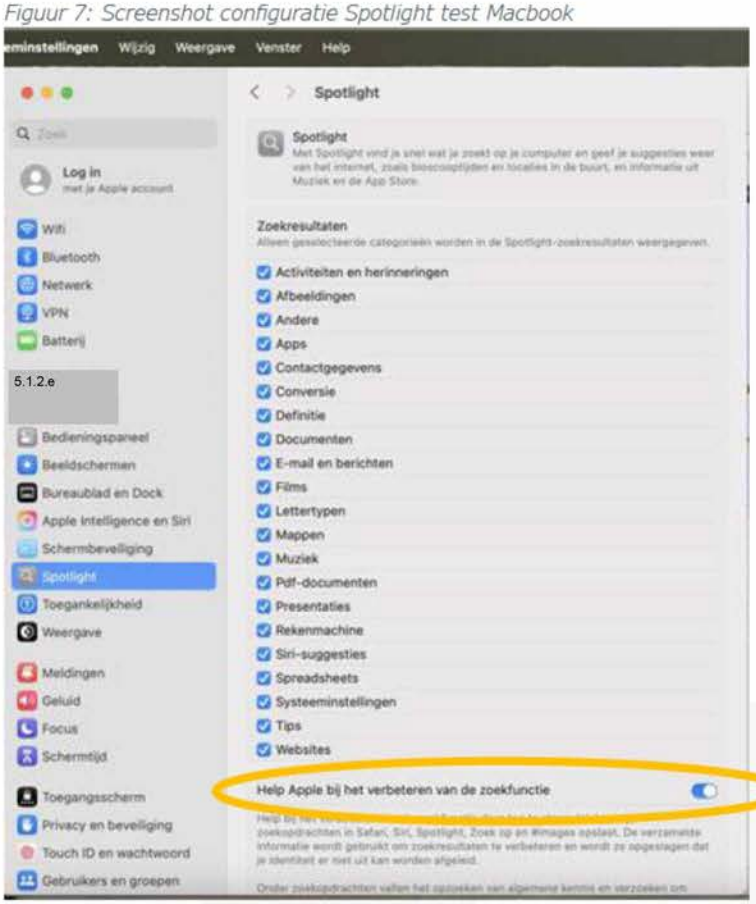
Docnr1

Figuur 6: Deel van ontvangen antwoord van Apple



Uit Figuur 7 blijkt dat SSC-ICT de optie aan heeft laten staan om Apple te helpen bij het verbeteren van de zoekfunctie.

Figuur 7: Screenshot configuratie Spotlight test Macbook

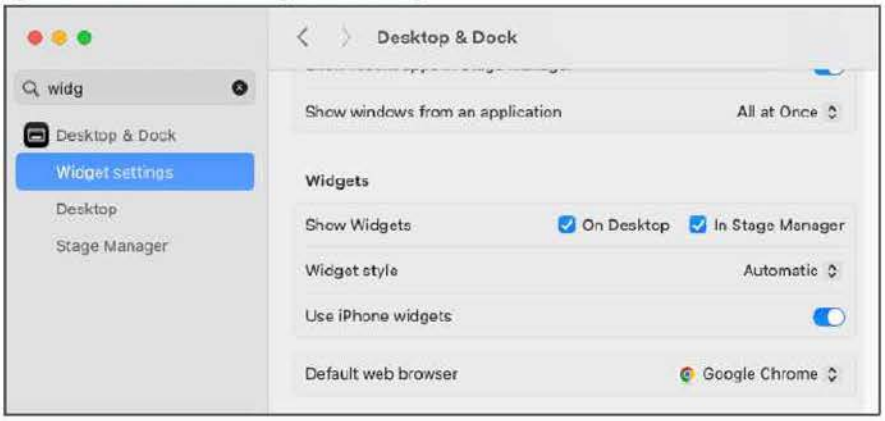


Het zevende domein (cdn2.smoot.apple.com) levert eventuele plaatjes aan die op internet staan, als die plaatjes voorkomen in de Spotlight resultaten. Een Spotlight zoekopdracht naar 'Floor' leidde bijvoorbeeld naar een URL met een foto van 5.1.2.e Maar in plaats van dat Apple dan dat plaatje rechtstreeks ophaalt bij die website (en daarmee het IP-adres van de werknemer doorgeeft), gebruikt Apple een eigen CDN om dat plaatje te serveren. Dat is een privacyvriendelijke feature, maar waarschijnlijk vooral ontworpen om de performance van Spotlight te optimaliseren.

Het achtste en negende domein (over beurskoersen en weer) zijn het gevolg van Widgets die standaard aanzet op macOS. Widgets zijn lichtgewicht applicaties die op de achtergrond blijven draaien. SCC-ICT kan deze widgets uitzetten. Zie Figuur 8 hieronder.

Docnr1

Figuur 8: User interface widgets bediening



Tabel 9: Netwerkeindpunten vanaf MacOS en manier van waarneming

	Netskope	Zonder Netskope	
Host	Wireshark	Wireshark	Mitmproxy
da-pr-ecslo-16vz8llff1sru-159561671.eu-central-1.elb.amazonaws.		✓	
wxt-registration-ingressgateway.acmhwxt-prd-1.prod.infra.webex.		✓	
wxt-registration-ingressgateway.acmhwxt-prd-4.prod.infra.webex.		✓	
wxt-registration-ingressgateway.afrawxt-prd-1.prod.infra.webex.		✓	
wxt-registration-ingressgateway.afrawxt-prd-2.prod.infra.webex.		✓	
epx-enterpriseproxy-1.d03-016.ic3-calling-enterpriseproxy.01-fr		✓	
epx-enterpriseproxy-2.d03-034.ic3-calling-enterpriseproxy.01-no		✓	
epx-enterpriseproxy.d03-036.ic3-calling-enterpriseproxy.01-nort		✓	
epx-enterpriseproxy.d03-014.ic3-calling-enterpriseproxy.01-swed		✓	
5.1.2.h	✓		
	✓		
	✓		
	✓		
		✓	
	✓		
	✓		
		✓	
	✓		
	✓		
	✓		
	✓		

5.1.2.h		✓	
		✓	
		✓	
		✓	
		✓	
		✓	
		✓	
		✓	
		✓	
		✓	
		✓	
		✓	
		✓	
		✓	
	sp-20191001060653164200000004-710657394.eu-west-1.elb.amazonaws	✓	
	token.safebrowsing.apple	✓	✓
	fritz.box	✓	
	Mac.fritz.box	✓	
	api.ipdata.co	✓	
	ingest.insights.ninetailed.co	✓	
	t.co	✓	
	app-site-association.g.aaplimg.com	✓	
	safebrowsing.g.aaplimg.com	✓	
	cdn.smoot.g.aaplimg.com	✓	
	smoot-searchv2-aeun1b.v.aaplimg.com	✓	
	user-sync.adhese.com	✓	
	ams3-ib.adnxs.com	✓	
	d.adroll.com	✓	
	ec2-18-210-229-244.compute-1.amazonaws.com	✓	
	ec2-52-71-121-170.compute-1.amazonaws.com	✓	
	ec2-34-251-7-23.eu-west-1.compute.amazonaws.com	✓	
	firewall-external-2134955858.eu-west-1.elb.amazonaws.com	✓	
	dt-external-217593033.us-east-1.elb.amazonaws.com	✓	
	s3-3-w.amazonaws.com	✓	

Docnr1

api.eu.amplitude.com	✓	
api-sr.eu.amplitude.com	✓	
sr-client-cfg.eu.amplitude.com	✓	
euc1-wps-prod.apple.com	✓	
help.apple.com	✓	✓
gsp-ssl.ls.apple.com	✓	✓
ocsp2.apple.com	✓	✓
api-glb-aeun1b.smoot.apple.com	✓	✓
cdn2.smoot.apple.com	✓	✓
stocks-data-service.apple.com	✓	✓
weatherkit.apple.com	✓	✓
a6370ebea231e0c9a.awsglobalaccelerator.com	✓	
ac99c40bc9e28338c.awsglobalaccelerator.com	✓	
onedsblobprdcus17.centralus.cloudapp.azure.com	✓	
onedsblobvmssprdcus02.centralus.cloudapp.azure.com	✓	
onedscolprdcus13.centralus.cloudapp.azure.com	✓	
onedscolprdeus09.eastus.cloudapp.azure.com	✓	
onedscolprdeus11.eastus.cloudapp.azure.com	✓	
onedscolprdeus22.eastus.cloudapp.azure.com	✓	
in1-gw2-01-3d6c3051.eastus2.cloudapp.azure.com	✓	
in1-gw2-04-3d6c3051.eastus2.cloudapp.azure.com	✓	
b-tr-teampb-frcn-01.francecentral.cloudapp.azure.com	✓	
onedscolprdfrc00.francecentral.cloudapp.azure.com	✓	
onedscolprdfrc01.francecentral.cloudapp.azure.com	✓	
onedscolprdfrc02.francecentral.cloudapp.azure.com	✓	
onedscolprdfrc04.francecentral.cloudapp.azure.com	✓	
onedscolprdfrc06.francecentral.cloudapp.azure.com	✓	
onedscolprdfrc07.francecentral.cloudapp.azure.com	✓	
osiprod-frc-flax-azsc-000.francecentral.cloudapp.azure.com	✓	
onedscolprdgwc00.germanywestcentral.cloudapp.azure.com	✓	
onedscolprdgwc05.germanywestcentral.cloudapp.azure.com	✓	
onedscolprdgwc06.germanywestcentral.cloudapp.azure.com	✓	
waws-prod-fra-037-8717.germanywestcentral.cloudapp.azure.com	✓	

mps-mde-prd-neu-14.northeurope.cloudapp.azure.com	✓
mps-mde-prd-neu-16.northeurope.cloudapp.azure.com	✓
nmoendpoint.northeurope.cloudapp.azure.com	✓
onedscolprdneu00.northeurope.cloudapp.azure.com	✓
onedscolprdneu01.northeurope.cloudapp.azure.com	✓
onedscolprdneu03.northeurope.cloudapp.azure.com	✓
onedscolprdneu06.northeurope.cloudapp.azure.com	✓
onedscolprdneu07.northeurope.cloudapp.azure.com	✓
onedscolprdneu08.northeurope.cloudapp.azure.com	✓
onedscolprdneu09.northeurope.cloudapp.azure.com	✓
onedscolprdneu10.northeurope.cloudapp.azure.com	✓
onedscolprdneu11.northeurope.cloudapp.azure.com	✓
onedscolprdneu12.northeurope.cloudapp.azure.com	✓
onedscolprdneu13.northeurope.cloudapp.azure.com	✓
onedscolprdneu14.northeurope.cloudapp.azure.com	✓
onedscolprdneu15.northeurope.cloudapp.azure.com	✓
osiprod-neu-bronze-azsc-000.northeurope.cloudapp.azure.com	✓
osiprod-neu-buff-azsc-000.northeurope.cloudapp.azure.com	✓
pexsucpeu01.northeurope.cloudapp.azure.com	✓
waws-prod-db3-193-f8da.northeurope.cloudapp.azure.com	✓
waws-prod-db3-239-40ad.northeurope.cloudapp.azure.com	✓
wd-prod-cp-eu-north-3-fe.northeurope.cloudapp.azure.com	✓
a-tr-teamsc-swcn-01.swedencentral.cloudapp.azure.com	✓
osiprod-swc-flax-azsc-000.swedencentral.cloudapp.azure.com	✓
pexsucpeu03.swedencentral.cloudapp.azure.com	✓
augloop-prod-pa00.westeurope.cloudapp.azure.com	✓
augloop-prod-pd02.westeurope.cloudapp.azure.com	✓
lb-traefik-ngs-production-client.westeurope.cloudapp.azure.com	✓
ns-prod-am3-512.westeurope.cloudapp.azure.com	✓
onedscolprdweu00.westeurope.cloudapp.azure.com	✓
onedscolprdweu01.westeurope.cloudapp.azure.com	✓
onedscolprdweu02.westeurope.cloudapp.azure.com	✓
onedscolprdweu03.westeurope.cloudapp.azure.com	✓

onedscolprdweu04.westeurope.cloudapp.azure.com	✓
onedscolprdweu05.westeurope.cloudapp.azure.com	✓
onedscolprdweu06.westeurope.cloudapp.azure.com	✓
onedscolprdweu07.westeurope.cloudapp.azure.com	✓
onedscolprdweu09.westeurope.cloudapp.azure.com	✓
onedscolprdweu10.westeurope.cloudapp.azure.com	✓
onedscolprdweu11.westeurope.cloudapp.azure.com	✓
onedscolprdweu12.westeurope.cloudapp.azure.com	✓
onedscolprdweu13.westeurope.cloudapp.azure.com	✓
onedscolprdweu14.westeurope.cloudapp.azure.com	✓
onedscolprdweu15.westeurope.cloudapp.azure.com	✓
osiprod-weu-bronze-azsc-000.westeurope.cloudapp.azure.com	✓
osiprod-weu-buff-azsc-000.westeurope.cloudapp.azure.com	✓
osiprod-weu-flax-azsc-000.westeurope.cloudapp.azure.com	✓
pexsucpeu02.westeurope.cloudapp.azure.com	✓
waws-prod-am2-417-e2e3.westeurope.cloudapp.azure.com	✓
wd-prod-cp-eu-west-1-fe.westeurope.cloudapp.azure.com	✓
wd-prod-cp-eu-west-3-fe.westeurope.cloudapp.azure.com	✓
onedsblobprdwus17.westus.cloudapp.azure.com	✓
onedscolprdwus18.westus.cloudapp.azure.com	✓
match.adsby.bidtheatre.com	✓
bitwarden.com	✓
tr.blismedia.com	✓
cdn.brandmetrics.com	✓
btloader.com	✓
api.btloader.com	✓
dsum-sec.casalemedia.com	✓
ds.ciscospark.com	✓
app.clearbit.com	✓
tag.clearbitscripts.com	✓
assets-tracking.crazyegg.com	✓
pagestates-tracking.crazyegg.com	✓
tracking.crazyegg.com	✓

gum.nl3.vip.prod.criteo.com	✓	
in-ftd-65.nl3.vip.prod.criteo.com	✓	
mug.nl3.vip.prod.criteo.com	✓	
ag.dns-finder.com	✓	
trackerapi.ebxcdn.com	✓	
star-mini.c10r.facebook.com	✓	
github.com	✓	
objects.githubusercontent.com	✓	
region1.google-analytics.com	✓	
adservice.google.com	✓	
ogads-pa.clients6.google.com	✓	
youtube-ui.l.google.com	✓	
ytimg.l.google.com	✓	
play.google.com	✓	
www.google.com	✓	
www.googleadservices.com	✓	
pagead2.googlesyndication.com	✓	
www.googletagmanager.com	✓	
5.1.2.h	✓	
5.1.2.h		✓
fonts.gstatic.com	✓	
www.gstatic.com	✓	
script.hotjar.com	✓	
static-cdn.hotjar.com	✓	
js.hs-banner.com	✓	
js.hs-scripts.com	✓	
perf-na1.hsforms.com	✓	
api.hubapi.com	✓	
track.hubspot.com	✓	
js-sec.indexww.com	✓	
neu-azsc-config.officeapps.live.com	✓	
nexusrules.officeapps.live.com	✓	✓
ocws-eu.officeapps.live.com	✓	✓

odc.officeapps.live.com	✓	✓
odc-eu.officeapps.live.com	✓	✓
euc.pptsgs.officeapps.live.com	✓	✓
roaming-eu.officeapps.live.com	✓	✓
uks-azsc-config.officeapps.live.com	✓	
ukw-azsc-config.officeapps.live.com	✓	
csp.microsoft.com	✓	✓
eu-mobile.events.data.microsoft.com	✓	✓
eu-office.events.data.microsoft.com	✓	✓
eu-teams.events.data.microsoft.com	✓	✓
mobile.events.data.microsoft.com	✓	✓
nw-umwatson.events.data.microsoft.com	✓	✓
graph.microsoft.com	✓	✓
agents.manage.microsoft.com	✓	✓
officeclient.microsoft.com	✓	✓
teams.microsoft.com	✓	✓
eu-prod.asyncgw.teams.microsoft.com	✓	✓
config.teams.microsoft.com	✓	✓
api.flightproxy.teams.microsoft.com	✓	✓
presence.teams.microsoft.com	✓	✓
go-eu.trouter.teams.microsoft.com	✓	✓
pub-ent-dewc-03-t.trouter.teams.microsoft.com	✓	✓
europe.cp.wd.microsoft.com	✓	✓
login.microsoftonline.com	✓	✓
ml314.com	✓	
in.ml314.com	✓	
survey-deploy.mopinion.com	✓	
dx.mountain.com	✓	
gs.mountain.com	✓	
px.mountain.com	✓	
opt.objectiveportal.com	✓	
augloop.office.com	✓	✓
westeurope-pa00.augloop.office.com	✓	✓

loki.delve.office.com	✓	✓
ecs.office.com	✓	✓
AMS-efz.ms-acdc.office.com	✓	
substrate.office.com	✓	✓
eop-g2.tm-4.office.com	✓	
outlook.office365.com	✓	✓
autodiscover-s.outlook.com	✓	✓
dataservice.protection.outlook.com	✓	✓
eur05.safelinks.protection.outlook.com	✓	✓
prod-autodetect.outlookmobile.com	✓	✓
global.px.quantserve.com	✓	
sb.scorecardresearch.com	✓	
dwrt1.sharepoint.com	✓	✓
eu-api.asm.skype.com	✓	✓
config.edge.skype.com	✓	✓
ingestion.smartocto.com	✓	
edge-web.dual-gslb.spotify.com	✓	
s.twitter.com	✓	
urbanlaurel.com	✓	
w.usabilla.com	✓	
js.usemessages.com	✓	
dev.visualwebsiteoptimizer.com	✓	
avatar-a.wbx2.com	✓	✓
board-a.wbx2.com	✓	✓
conv-a.wbx2.com	✓	✓
directory-search-a.wbx2.com	✓	✓
encryption-a.wbx2.com	✓	✓
feature-broadcast-b.wbx2.com	✓	✓
idbroker-guest-a.wbx2.com	✓	✓
llm1-connection-k.wbx2.com	✓	✓
locus-b.wbx2.com	✓	✓
mercury-connection-partition2-a.wbx2.com	✓	✓
metrics-a.wbx2.com	✓	✓

proximity-a.wbx2.com		✓	✓
wdm-a.wbx2.com		✓	✓
binaries.webex.com		✓	✓
global-nebulab-jfk02-dfw01.webex.com		✓	
global-utsa.webex.com		✓	
idbroker.webex.com		✓	✓
wxt-ci-ingressgateway.acmhwxt-prd-1.prod.infra.webex.com		✓	
wxt-general-ingressgateway.acmhwxt-prd-1.prod.infra.webex.com		✓	
wxt-message-ingressgateway.acmhwxt-prd-1.prod.infra.webex.com		✓	
wxt-ci-ingressgateway.acmhwxt-prd-2.prod.infra.webex.com		✓	
wxt-general-ingressgateway.acmhwxt-prd-2.prod.infra.webex.com		✓	
wxt-mercury-ingressgateway.acmhwxt-prd-2.prod.infra.webex.com		✓	
wxt-wxid-ingressgateway.acmhwxt-prd-3.prod.infra.webex.com		✓	
wxt-mercury-ingressgateway.acmhwxt-prd-4.prod.infra.webex.com		✓	
wxt-mercury-ingressgateway.afrawxt-prd-1.prod.infra.webex.com		✓	
wxt-ci-ingressgateway.afrawxt-prd-2.prod.infra.webex.com		✓	
wxt-meet-ingressgateway.apdxwxt-prd-2.prod.infra.webex.com		✓	
calliope-anycast.prod.infra.webex.com		✓	
xlm36.public.sa-01wrtm2.prod.infra.webex.com	✓		
xlm8.public.sa-01wrtm2.prod.infra.webex.com	✓		
xlm34.public.sa-02wrtm2.prod.infra.webex.com	✓		
xlm4.public.sa-02wrtm2.prod.infra.webex.com	✓		
xlm49.public.wamsm-a-0.prod.infra.webex.com	✓		
xlm13.public.wamsm-a-7.prod.infra.webex.com	✓		
xlm68.public.wamsm-a-7.prod.infra.webex.com		✓	
xlm41.public.wbomm-a-1.prod.infra.webex.com	✓		
xlm88.public.wbomm-a-1.prod.infra.webex.com	✓		
xlm140.public.wdfwm-a-1.prod.infra.webex.com	✓		
external-large-media64.public.wdfwm-a-11.prod.infra.webex.com	✓		
xlm6.public.wfram-a-1.prod.infra.webex.com	✓		
xlm101.public.wfram-a-8.prod.infra.webex.com	✓		
xlm125.public.wfram-a-8.prod.infra.webex.com	✓		
xlm13.public.wjfkm-a-14.prod.infra.webex.com	✓		

xlm181.public.wjfkm-a-14.prod.infra.webex.com	✓		
xlm123.public.wlhrm-a-5.prod.infra.webex.com	✓		
xlm145.public.wlhrm-a-5.prod.infra.webex.com	✓		
xlm36.public.wsjcm-a-6.prod.infra.webex.com	✓		
xlm14.public.wsjcm-a-8.prod.infra.webex.com	✓		
join-test.webex.com		✓	✓
reachable.webex.com		✓	✓
prod-achm-general.svc.webex.com		✓	✓
tsa.webex.com		✓	✓
avatar-prod-us-east-2.webexcontent.com		✓	✓
loki-loki2.s01-059.substrate-fast-loki.01-westeurope-prod.cosmi		✓	
officemru.x01-003.oxo-oasisice-mru.01-francecentral-prod.cosmic		✓	
partition-cname-trouter-ic3-edf-trouter-service-trouter-1.d02-0		✓	
partition-cname-trouter-ic3-edf-trouter-service-trouter-2.d02-0		✓	
cloud.ccm19.de		✓	
cdn.pdst.fm		✓	
ep1.adtrafficquality.google		✓	
ep2.adtrafficquality.google		✓	
surveystats.hotjar.io		✓	
vc-live-cf.hotjar.io		✓	
o4506026096263169.ingest.sentry.io		✓	
in.appcenter.ms		✓	✓
s0.2mdn.net		✓	
ad-delivery.net		✓	
www.tm.a.prd.aadg.akadns.net		✓	
track.adformnet.akadns.net		✓	
www.tm.prd.ags.akadns.net		✓	
prod.nexusrules.live.com.akadns.net		✓	
neu.pptsgs.live.com.akadns.net		✓	
eu-nw-courier-4.push-apple.com.akadns.net		✓	
eudbipv4.clients.config.office.akadns.net		✓	
a1091.dscapi7.akamai.net		✓	
a2047.dscapi9.akamai.net		✓	

a937.dscb.akamai.net		✓	
a1813.dscd.akamai.net		✓	
a1817.dscd.akamai.net		✓	
a360.dscd.akamai.net		✓	
a390.dscd.akamai.net		✓	
e212585.b.akamaiedge.net		✓	
e11408.d.akamaiedge.net		✓	
e119.dsca.akamaiedge.net		✓	
e2867.dsca.akamaiedge.net		✓	
e184071.dscb.akamaiedge.net		✓	
e212585.dscb.akamaiedge.net		✓	
e27429.dscb.akamaiedge.net		✓	
e28241.dscb.akamaiedge.net		✓	
e67691.dscb.akamaiedge.net		✓	
e127270.dscd.akamaiedge.net		✓	
e77980.dscd.akamaiedge.net		✓	
e673.dsce9.akamaiedge.net		✓	
e3528.dscg.akamaiedge.net		✓	
e6913.dscx.akamaiedge.net		✓	
e86303.dscx.akamaiedge.net		✓	
e10883.g.akamaiedge.net		✓	
e12627.g.akamaiedge.net		✓	
e6603.g.akamaiedge.net		✓	
api.apple-cloudkit.fe2.apple-dns.net	✓		
gateway.fe2.apple-dns.net		✓	
ax-0001.ax-dc-msedge.net		✓	
ax-0002.ax-dc-msedge.net		✓	
ax-0001.ax-msedge.net		✓	
officecieu.azurewebsites.net		✓	✓
realtime-tentacles-production.b-cdn.net		✓	
user-data-eu.bidswitch.net		✓	
script.crazyegg.com.cdn.cloudflare.net		✓	
kit.fontawesome.com.cdn.cloudflare.net		✓	

Docnr1

q.quora.com.cdn.cloudflare.net	✓
cdn.jsdelivr.net.cdn.cloudflare.net	✓
d162h6x3rxav67.cloudfront.net	✓
d16t1nucl0wcte.cloudfront.net	✓
d21y75miwcfqoq.cloudfront.net	✓
d2f5rvg67fro0x.cloudfront.net	✓
d2xvo51pr40ne7.cloudfront.net	✓
d3l8kopw1d3uiv.cloudfront.net	✓
d3orhvfyxudxxq.cloudfront.net	✓
d96vky0xjhjcq.cloudfront.net	✓
d9xp6exb8m82.cloudfront.net	✓
dzfq4ouujrxm8.cloudfront.net	✓
t.contentsquare.net	✓
assets.ctfassets.net	✓
ad.doubleclick.net	✓
googleads.g.doubleclick.net	✓
s-0005.dual-s-dc-msedge.net	✓
s-0005.dual-s-msedge.net	✓
h2.shared.global.fastly.net	✓
dualstack.n.sni.global.fastly.net	✓
amplitude.map.fastly.net	✓
h3.apis.apple.map.fastly.net	✓
prod.appnexus.map.fastly.net	✓
linkedin.map.fastly.net	✓
reddit.map.fastly.net	✓
dualstack.reddit.map.fastly.net	✓
platform.twitter.map.fastly.net	✓
vimeo.map.fastly.net	✓
s-part-0039.t-0009.fb-t-msedge.net	✓
scontent.xx.fbcdn.net	✓
js.hs-analytics.net	✓
js.hsadspixel.net	✓
forms.hscollectedforms.net	✓

js.hsforms.net		✓	
l-0007.l-msedge.net		✓	
ln-0002.ln-msedge.net		✓	
ipv4.ln-0004.ln-msedge.net		✓	
features.netscalergateway.net		✓	✓
statics.teams.cdn.office.net		✓	✓
clients.config.office.net		✓	✓
support.content.office.net		✓	✓
s-0005.s-msedge.net		✓	
s-0006.s-msedge.net		✓	
sync.sxp.smartclip.net		✓	
dual-spo-0005.spo-msedge.net		✓	
s-part-0039.t-0009.t-msedge.net		✓	
www.tm.a.prd.aadg.trafficmanager.net		✓	
beta-autodetect.outlookmobile.com.trafficmanager.net		✓	
cosmic-francecentral-ns-1d4296700e95.trafficmanager.net		✓	
cosmic-swedencentral-ns-dfecc19aa9d5.trafficmanager.net		✓	
cosmic-westeurope-ns-63ee9b9a4ec7.trafficmanager.net		✓	
web.blz22prdstr01a.store.core.windows.net		✓	
officewhatsnew.z13.web.core.windows.net		✓	✓
citrixtelemetryeheu-alias.servicebus.windows.net		✓	✓
www.google.nl		✓	
minbzk.nl		✓	
5.1.2.h		✓	
www.rijksoverheid.nl		✓	
5.1.2.h		✓	
stats.thuisarts.nl		✓	
www.thuisarts.nl		✓	
ade.weborama.nl		✓	
mrq.weborama.nl		✓	
5.1.2.h	✓		
5.1.2.h		✓	
cdn.cookielaw.org		✓	

secure.eicar.org	✓
5.1.2.h	✓
edge-cloudmessaging-access-point-aks-prod-westeurope.westeurope	✓

3.2.2 Geobserveerde protocollen

3.2.2.1 DNS (poort 53)

Tijdens het testen is (net als op Windows) alleen DNS-verkeer geobserveerd naar een DNS resolver op het lokale netwerk. Op een vertrouwd netwerk vormt dit verkeer geen ongebruikelijk risico. Maar op onvertrouwde netwerken, bij medewerkers thuis, of onderweg in hotels of cafés, kan dat betekenen dat de domeinnamen waarmee de medewerker verbinding maakt uitlekken.

3.2.2.2 HTTP (poort 80)

Vrijwel al het web-verkeer gaat tegenwoordig over een versleutelde verbinding (HTTPS). Toch is er tijdens het testen een niet-versleutelde HTTP verbinding opgemerkt buiten het lokale netwerk naar het Akamai CDN dat verzoeken afhandelt voor Entrust OCSP.[12] Het verzoek bevat een UUID, een unieke user id met een versleutelde inhoud.

Figuur 9: Inhoud verkeer naar Entrust OCSP

Tabel 10: Aantal ontvangen en verzonden bytes bericht naar Akamai CDN

Host	Verzonden Bytes	Ontvangen Bytes
e6913.dscx.akamaiedge.net	874	2385

[12] https://en.wikipedia.org/wiki/Online_Certificate_Status_Protocol

3.2.2.3 Poort 88 (Kerberos?)

Tijdens het testen is alleen Kerberos-verkeer geobserveerd naar een eindpunt op het lokale netwerk. Kerberos is een authenticatie-protocol. Het ging om een enkel TCP SYN pakket bedoeld om een verbinding op te zetten tijdens de test met Netskope.

3.2.2.4 RTP (poort 5004)

RTP is het Realtime Transport Protocol, een protocol dat onder andere wordt gebruikt voor het streamen van audio en video. Cisco gebruikt dit protocol voor Webex. Er zijn geen Teams berichten via deze poort verzonden.

Tabel 11: RTP-berichten met verzonden en ontvangen bytes

Host	Verzonden Bytes	Ontvangen Bytes
xlm36.public.sa-01wrtm2.prod.infra.webex.com	1242	1310
xlm8.public.sa-01wrtm2.prod.infra.webex.com	1242	1310
xlm34.public.sa-02wrtm2.prod.infra.webex.com	1242	1310
xlm4.public.sa-02wrtm2.prod.infra.webex.com	1242	1310
xlm49.public.wamsm-a-0.prod.infra.webex.com	1242	1634
xlm13.public.wamsm-a-7.prod.infra.webex.com	1242	1742
xlm68.public.wamsm-a-7.prod.infra.webex.com	78	370
xlm41.public.wbomm-a-1.prod.infra.webex.com	1176	1268
xlm88.public.wbomm-a-1.prod.infra.webex.com	1242	1202
xlm140.public.wdfwm-a-1.prod.infra.webex.com	1176	920
external-large-media64.public.wdfwm-a-11.prod.infra.webex.com	1242	1052
xlm6.public.wfram-a-1.prod.infra.webex.com	1146	746
xlm101.public.wfram-a-8.prod.infra.webex.com	1146	812
xlm125.public.wfram-a-8.prod.infra.webex.com	1068	1202
xlm13.public.wjfkm-a-14.prod.infra.webex.com	1242	1244
xlm181.public.wjfkm-a-14.prod.infra.webex.com	1242	1310
xlm123.public.wlhrm-a-5.prod.infra.webex.com	1080	878
xlm145.public.wlhrm-a-5.prod.infra.webex.com	1176	1574

xlm36.public.wsjcm-a-6.prod.infra.webex.com	1242	854
xlm14.public.wsjcm-a-8.prod.infra.webex.com	1176	920

3.2.2.5 XMPP (poort 5223)

XMPP is het Extensible Messaging and Presence Protocol, dat wordt gebruikt voor onder andere chat en pushberichten.

Host	Verzonden Bytes	Ontvangen Bytes
eu-nw-courier-4.push-apple.com.akadns.net	684	360

Tabel 12: XMPP berichten met verzonden en ontvangen bytes

3.2.3 Geobserveerde cookies

Op de Macbook zijn precies dezelfde testhandelingen verricht als op de Windows laptop, en zijn dezelfde vier websites bezocht. In de lijst met geobserveerde netwerk eindpunten zijn dezelfde advertentie netwerken en tracking partijen zichtbaar als op Windows. Toch zijn er in de Safari browser op de Macbook aanzienlijk minder cookies geplaatst dan in Edge op Windows. Dat kan twee oorzaken hebben: ofwel het was moeilijker om dit verkeer goed te onderscheppen door ingebouwde privacybescherming in MacOS, of de Safari browser was strakker ingesteld om tracking cookies te weren.

Tabel 13:Hosts and geplaatste cookies

Host	Cookies
eu-prod.asyncgw.teams.microsoft.com	skypetoken_asm platformid_asm
login.microsoftonline.com	Fpc ESTSAUTHPERSISTENT Buid MSFPC Brcap MicrosoftApplicationsTelemetryDeviceId x-ms-gateway-slice stsservicecookie
outlook.office365.com	exchangecookie
eur05.safelinks.protection.outlook.com	Policy expires path SameSite secure httponly
eu-api.asm.skype.com	skypetoken_asm platformid_asm

idbroker.webex.com	JSESSIONID amlbcookie amlbcookiesm wxidIstio
join-test.webex.com	wbx
officecieu.azurewebsites.net	ARRAffinity ARRAffinitySameSite