Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

DNS-monitoring wordt moeilijker

Wees voorbereid op de modernisering van transportprotocollen

Factsheet FS-2019-01 | versie 1.0 | 30 september 2019

Nieuwe DNS-transportprotocollen (DoH, DoT) maken het moeilijker om DNS-verzoeken te monitoren of aan te passen. Dat is waardevol, omdat netwerken vaak niet te vertrouwen zijn. Tegelijkertijd kan het bestaande beveiligings-maatregelen ineffectief maken, interne naamgeving onthullen of connectiviteit onderbreken. Deze negatieve bijverschijnselen zijn nauwelijks te mitigeren op netwerkniveau. Ze vereisen mitigatie in DNS-infrastructuur en op individuele apparaten.
Het NCSC adviseert organisaties om voorkeurs-(DNS-)resolvers aan te wijzen, deze te configureren op alle apparaten onder beheer, en kennis te nemen van de beschikbare moderne DNS-transportmethoden.

Achtergrond

DNS is een van de belangrijkste protocollen in het fundament van het internet. Toegenomen zorgen over monitoring van DNS-verkeer door ISP's heeft geleid tot de standaardisatie van moderne DNS-transportprotocollen ('DNS-transporten'), die gebruik maken van versleuteling. Met een DNS-transport wisselen een endpoint en de recursive caching nameserver van het endpoint ('resolver') DNS-verzoeken en -antwoorden uit. Gebruikers die willen dat hun ISP hun DNS-verzoeken niet kan lezen, kunnen een versleuteld DNS-transport gebruiken. Ze gebruiken daarbij een resolver bij een derde partij, waardoor hun ISP geen enkele rol meer speelt in het afhandelen van hun DNS-verzoeken.

Doelgroep

Systeem- of netwerkbeheerders en securityofficers.

Wat is er aan de hand?

Versleuteld DNS-transporten worden populairder

Systeem- of netwerkbeheerders en securityprofessionals zijn gewend dat DNS-verkeer onversleuteld naar poort 53 (tcp en udp) gaat. Recentelijk zijn er nieuwe DNS-transporten gestandaardiseerd waarbij encryptie wordt gebruikt om vertrouwelijkheid en integriteit te bieden in de aanwezigheid van een kwaadwillende op het netwerk.

De belangrijkste feiten

1. Moderne DNS-transporten, die gebruikmaken van versleuteling worden populairder.
2. Steeds meer software maakt niet langer gebruik van DNS-resolving op systeemniveau. Uw organisatie kan onbewust verantwoordelijkheid voor DNS-resolving aan een derde partij uit handen hebben gegeven.
3. Dit kan als gevolg hebben dat beveiligingsmaatregelen ineffectief worden, interne naamgeving onthuld wordt of connectiviteit onderbroken wordt.

Deze nieuwe DNS-transporten worden populairder om DNS-verkeer te transporteren tussen endpoints en de recursive caching name server ('resolver') die geconfigureerd is op de endpoints.

DNS over TLS (DoT)[1] transporteert DNS-verkeer over een TLS-tunnel op tcp/853. DNS over HTTPS (DoH)[2] transporteert DNS-verkeer over een https-verbinding op tcp/443. Beiden kunnen vertrouwelijkheid en integriteit bieden in de aanwezigheid van een actieve aanvaller op het netwerk.[3] Het is waarschijnlijk dat toekomstige transportprotocollen, zoals QUIC, ook gebruikt gaan worden om DNS-verkeer te transporteren met nuttige beveiligingseigenschappen.

Populaire besturingssystemen hebben (nog) geen meegeleverde ondersteuning voor de nieuwe versleutelde DNS-transporten, met als uitzondering Android. Android 9 Pie kiest ervoor om onversleuteld DNS-verkeer over tcp/udp poort 53 naar DoT te upgraden wanneer de resolver dit ondersteunt.[4] Dit opportunistische gebruik van DoT biedt vertrouwelijkheid in de aanwezigheid van een passieve observator op het netwerk, maar beschermt niet tegen een actieve aanvaller.

Steeds meer software maakt niet langer gebruik van DNS-resolving op systeemniveau

Applicatie-ontwikkelaars gebruikten jarenlang de softwarebibliotheken die met verschillende besturingssystemen mee werden geleverd om hun DNS-resolving te doen. Verschillende applicaties gebruikten zo één enkele DNS-stub-resolver (op systeemniveau). De configuratie van deze resolver bepaalde voor het hele systeem waar DNS-verzoeken naartoe werden gestuurd.

Sommige applicatie-ontwikkelaars hebben de functionaliteit voor DNS-resolving direct in hun applicatie ingebouwd. Dit stelt ze in staat om gebruik te maken van de voordelen van nieuwe versleutelde DNS-transporten, zonder dat het besturingssysteem deze ondersteunt. De ontwikkelaar kan dan zelf bepalen welke resolver de applicatie gebruikt. Verschillende ontwikkelaars maken van deze mogelijkheid gebruik. DNS-verzoeken van deze applicaties gaan dus niet meer naar de DNS-resolver die op systeemniveau is ingesteld.

Mozilla levert in Firefox eigen functionaliteit voor DNS-resolving mee, die ook DoH ondersteunt. Mozilla experimenteert in de VS[5] met een Firefox-configuratie die DNS-verzoeken naar Cloudflare stuurt. Google experimenteert in Chrome wereldwijd[6] met DoH-functionaliteit die DNS-verzoeken over DoH stuurt wanneer de DNS-resolver die op systeemniveau wordt gebruikt in een whitelist staat van partijen die DoH ondersteunen.

Handelingsperspectief

- Wijs voorkeurs-(DNS-)resolvers aan.
- Configureer deze voorkeursresolvers op alle apparaten onder beheer.
- Neem kennis van de beschikbare moderne DNS-transporten.

Wat betekent dit voor mijn organisatie?

Ineffectieve beveiligingsmaatregelen

Organisaties die vertrouwen op de mogelijkheid om onversleuteld DNS-verkeer te kunnen inspecteren zullen na verloop van tijd hun inzicht zien afnemen. Organisaties die security-monitoring of filtering doen op de resolvers die zijn geconfigureerd op systeemniveau zullen merken dat deze maatregelen ineffectief worden zodra applicaties een andere DNS-resolver gaan gebruiken.

Informatie lekken en onthullen van interne naamgevingen

DNS-verzoeken kunnen veel gevoelige informatie bevatten, waaronder bezochte websites en bestemmingen van e-mail. Veel organisaties beschouwen DNS-records voor interne systemen en netwerken als gevoelige informatie.

De keuze voor een resolver is een kwestie van vertrouwen. Wanneer apparaten onder beheer gebruik gaan maken van resolvers die door derde partijen worden beheerd, zullen deze resolvers ook DNS-verzoeken gaan verwerken die gevoelige informatie bevatten. Afhankelijk van het vertrouwen in deze derde partijen en de juridische context waarin deze partijen opereren, kan dit een risico vormen.

Onderbreking connectiviteit

Organisaties die de zichtbaarheid van naamgeving van interne resources beperkt hebben tot interne netwerken, lopen een risico wanneer apparaten gebruik gaan maken van resolvers van derde partijen. De derde partij zal geen antwoord kunnen geven op DNS-verzoeken voor interne resource records als deze antwoorden niet gegeven kunnen worden door uw

[1] DNS over TLS staat beschreven in RFC 7858, beschikbaar op https://datatracker.ietf.org/doc/rfc7858/
[2] DNS over HTTPS staat beschreven in RFC 8484, beschikbaar op https://datatracker.ietf.org/doc/rfc8484/
[3] Het endpoint vereist hiervoor een hostname van de resolver, die wordt gebruikt voor TLS-authenticatie. Zie voor meer informatie sectie 6.6 van RFC 8310, beschikbaar op https://datatracker.ietf.org/doc/rfc8310/

[4] Bron: https://android-developers.googleblog.com/2018/04/dns-over-tls-support-in-android-p.html
[5] Bron: https://blog.mozilla.org/futurereleases/2019/09/06/whats-next-in-making-dns-over-https-the-default/
[6] Bron: https://www.chromium.org/developers/dns-over-https

authoritative nameservers op het publieke internet. Dit kan leiden tot connectiviteitsproblemen op interne netwerken en VPN's.

Wat adviseert het NCSC?

Het NCSC raadt organisaties aan om voorkeursresolvers aan te wijzen en deze op apparaten onder beheer te configureren. Overweeg om DoT of DoH in te schakelen en te gebruiken op de voorkeursresolvers wanneer dit wordt ondersteund. Dit advies staat nader uitgewerkt in tabel 1.

Accepteer of mitigeer risico's op uw netwerken voor apparaten die niet onder eigen beheer vallen, zoals internettoegang voor bezoekers of privé-apparaten. Dit advies staat nader uitgewerkt in tabel 2.

Tot slot

Zolang er op beperkte schaal wordt geexperimenteerd met DoH en Dot is er tijd voor voorbereiding. De trend is echter duidelijk: DNS-monitoring wordt moeilijker.

Om DNS-monitoring als maatregel effectief te houden, zal het nodig zijn om aanpassingen te maken op uw endpoints en in uw eigen DNS-infrastructuur. Waar het tot nu toe mogelijk was om DNS-monitoring op een centraal punt in het netwerk uit te voeren, zal een gecentraliseerde aanpak in de toekomst steeds minder opleveren.

Hoe lang gecentraliseerde DNS-monitoring nog een effectieve maatregel blijft, is sterk afhankelijk van de snelheid waarmee Mozilla en Google ondersteuning in hun software activeren. Als u vandaag begint met het aanpassen van uw DNS-monitoring, dan wordt u niet verrast door de naderende veranderingen.

Tabel 1 Gebruik voorkeursresolvers voor apparaten onder beheer

Bepaal waar u wilt dat clients hun DNS-verzoeken naartoe sturen

- Beheert u uw eigen resolvers of is dit uitbesteed aan een derde partij?
- Wat zijn de gevolgen wanneer clients gebruikmaken van een niet-voorkeursresolver? Beschouw:
  a. vertrouwelijkheid van de queries;
  b. DNS-zones die niet te resolven zijn vanaf het publieke internet (split-horizon DNS);
  c. performance en beschikbaarheid;
  d. beveiligingsmaatregelen, zoals DNS-filteren of security-monitoring;
  e. zicht voor performance-metingen of foutopsporing.

Begrijp hoe clients die onder eigen beheer vallen weten waar ze hun DNS-verzoeken naartoe moeten sturen

- Begrijp hoe DNS-configuratie op systeemniveau wordt ingesteld binnen uw organisatie.
  a. De meeste netwerken bieden resolver-configuratie aan met een DHCP-optie.
  b. Netwerk-flow-data kan u helpen begrijpen welke resolvers in gebruik zijn binnen uw organisatie.
- Begrijp welke applicaties[7] met alternatieve resolvers zijn uitgerust. Denk aan:
  a. webbrowsers en plugins;
  b. apps op mobiele apparaten;

Stel resolver-configuratie in op clients als hun standaardconfiguratie dit vereist

- Mozilla Firefox levert zogeheten policy knobs om DoH in/uit te schakelen en om een voorkeursresolver op te geven.[8] Mozilla zegt dat DoH standaard uit staat wanneer enterprise roots zijn geïnstalleerd[9] voor TLS-interceptie[10].
- Google Chrome zal ook policy knobs leveren om DoH in/uit te schakelen en een voorkeursresolver op te geven.[11]

Tabel 2 Accepteer of mitigeer beperkte zichtbaarheid van DNS-verzoeken van apparaten die niet onder eigen beheer vallen

Veel organisaties bieden internettoegang aan voor bezoekers of privé-apparaten. De apparaten op deze netwerken zijn niet onder beheer van de organisatie. Er is dan ook geen invloed op de gebruikte resolver-configuratie. Na verloop van tijd is het aannemelijk dat apparaten hun DNS-verzoeken zullen versleutelen, kiezen voor niet-voorkeursresolvers van de organisatie, of beiden.

- Wees bewust van het feit dat alle beveiligingsmaatregelen die afhankelijk zijn van zicht op DNS-verkeer na verloop van tijd afnemen in effectiviteit.
- Sommige applicaties maken mitigatie op netwerkniveau mogelijk, maar de ondersteuning hiervoor kan (bij misbruik) op korte termijn eindigen.
  a. Mozilla Firefox staat netwerken toe om aan te geven dat er gebruik gemaakt wordt van DNS-filtering op resolver-niveau door middel van een zogeheten canary domain.[9]
- Houd rekening met het niveau van toegang dat aan apparaten wordt gegeven die niet onder eigen beheer vallen, de risico's die dit met zich meebrengt en de benodigde afweging voor gast- en privé-gebruik wanneer u kiest voor het accepteren ofwel mitigeren van beperkt zicht.

[7] Zie bijvoorbeeld https://en.wikipedia.org/wiki/DNS_over_HTTPS#Client_support en https://dnsprivacy.org/wiki/display/DP/DNS+Privacy+Clients
[8] Een overzicht van beschikbare policy knobs is beschikbaar op https://github.com/mozilla/policy-templates/blob/master/README.md#dnsoverhttps
[9] Bron: https://support.mozilla.org/en-US/kb/configuring-networks-disable-dns-over-https
[10] Zie ook de factsheet TLS-interceptie van het NCSC, beschikbaar op https://www.ncsc.nl/documenten/factsheets/2019/juni/01/factsheet-tls-interceptie
[11] Deze staan beschreven in de designdocumentatie, beschikbaar op https://www.chromium.org/developers/dns-over-https

Uitgave
Nationaal Cyber Security Centrum (NCSC)
Postbus 117, 2501 CC Den Haag
Turfmarkt 147, 2511 DP Den Haag
070 751 5555

Meer informatie
www.ncsc.nl
info@ncsc.nl
@ncsc_nl

FS-2019-01 | versie 1.0 | 30 september 2019