Privacypolicy

Resolver Reputation 1.0

Datum
17 maart 2015

Classificatie
Publiek

Auteur
SIDN Labs

Blad
1/2

Contact
T 026 352 55 00
support@sidn.nl
www.sidn.nl

Bezoekadres
Meander 501
6825 MD Arnhem

Postadres
Postbus 5022
6802 EA Arnhem

Naam onderzoek/applicatie	Resolver Reputation 1.0
Ingangsdatum policy	2015-03-17
Doel van de applicatie of het onderzoek	De veiligheid en betrouwbaarheid van .nl (en het internet in het algemeen) verhogen door onderzoek te doen naar het toekennen van een reputatie aan resolvers. Aan de hand van deze reputatie kunnen bepaalde vormen van abuse worden bestreden. Concreet gaat het hier om de bestrijding van botnet-clients die spam versturen (zogenaamde spambot). Deze clients worden op basis van specifieke DNS-gedragskenmerken door het systeem gedetecteerd en hun IP-adressen worden kenbaar gemaakt aan de Abuse Information Exchange, voor verdere verwerking. Die verwerking bestaat uit het doorzetten van het IP-adres naar de ISP in kwestie, die daarop desgewenst passende maatregelen kan nemen. Uiteindelijk is het concrete doel (binnen de context van deze aanvraag) dat het aantal met spambot-malware geïnfecteerde pc's in Nederland afneemt.
Persoonsgegevens	IPv4- en IPv6-adressen van alle systemen die DNS-verzoeken doen naar .nl-domeinen en ook een tijdsindicatie van het meest recent waargenomen DNS-verzoek.
Grondslag	De grondslag voor de verwerking is gerechtvaardigd belang.
Filters	IP-adressen die langere tijd (momenteel 1 maand) niet meer worden gezien, worden verwijderd uit de database.

	Daadwerkelijke query-data is in de huidige versie van ResRep niet relevant en wordt weggelaten. Er wordt alleen naar meta-informatie gekeken (bijvoorbeeld: wordt er om MX-records gevraagd, is het RD-bit gezet, is er sprake van veel NX-domains?)
Retentie	In de huidige versie van ResRep blijft het IP-adres bewaard zolang we deze voorbij zien komen op de ns1.dns.nl. Pas als deze langere tijd niet meer voorbij komt, verdwijnt hij automatisch uit de database.
Toegang	Alle medewerkers van SIDN Labs. De data staat op dit moment op een server die is beschermd middels persoonsgebonden 2F-authenticatie (TOTP voor SSH en client-certificaten voor web, naast username wachtwoord combinatie).
Publicatie/delen	IP-adressen waarvan wordt vastgesteld dat deze gedragskenmerken hebben van een met spambot-malware geïnfecteerd systeem, worden met een interval van 30 minuten en geautomatiseerd gerapporteerd aan de AbuseHub. Ook wordt een zogenaamde timestamp meegegeven van de tijd waarop dat IP-adres (binnen de betreffende 30 minuten interval) voor het laatst het gezochte gedragskenmerk vertoonde. Alle overige details worden achterwege gelaten en niet gedeeld met de AbuseHub. We doen dit op voorwaarde dat tussen SIDN en de AbuseHub een overeenkomst wordt gesloten die inhoudelijk overeenkomt met een bewerkersovereenkomst. De AbuseHub is gevestigd in Nederland.
Type	Productie
Andere beveiligingsmaatregelen	Geen