Privacypolicy

Joint Threat Intelligence Enrichment

Datum
01 augustus 2017

Classificatie
Publiek

Auteur
SIDN Labs

Blad
1/3

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	Joint Threat Intelligence Enrichment (JTIE)
Ingangsdatum policy	01-08-2017
Doel van de applicatie of het onderzoek	Het doel van JTIE is een mechanisme te ontwikkelen dat de 'threat intelligence' van de Fraudehelpdesk (FHD) en SIDN over .nl-domeinnamen combineert en zo beide partijen in staat stelt domeinnamen met een hogere accuratesse als verdacht te classificeren. Daarmee willen we uiteindelijk het internet veiliger maken. Daarbij ontvangt SIDN van FHD .nl-domeinnamen, die in mails voorkomen die FHD gebruikers melden. Voor elke domeinnaam stuurt SIDN de volgende data aan FHD terug: aantal DNS-queries laatste 7 dagen, registratiedatum, een registrar-pseudoniem. Nederlandse registrant (ja/nee) wordt niet meer gedeeld. Aanvullend ontvangt SIDN nu van FHD een lijst met URL's van .nl-domeinnamen in plaats van alleen de 2nd level domeinnamen. Na de evaluatie van FHD stuurt FHD feedback terug naar SIDN, of FHD de mail als malafide classificeert. Dit bepaalt FHD op basis van de data van SIDN en andere bronnen.
Persoonsgegevens	Voor elke domeinnaam verwerkt SIDN de volgende persoonsgegevens: Aantal DNS-queries van de laatste 7 dagen, registrarnaam, domeinnamen van URL's die in een verdachte mail staan. Daarvoor moet SIDN de DNS-queries verwerken die ook IP-adressen bevatten. Een pseudoniem van de naam van de

registrar is relevant omdat malafide domeinnamen vaak bij registrars geregistreerd zijn die bekend zijn om malafide domeinnaamregistraties. Als persoonsgegevens in URLs staan, anonimiseert FHD deze voordat FHD de URL met SIDN deelt.

Grondslag

De grondslag voor de verwerking is gerechtvaardigd belang.

Bestaand onderzoek maakt duidelijk dat een flinke groei van het aantal DNS-queries een indicatie voor domeinnaammisbruik is. De registratiedatum is relevant om onderscheid te maken tussen een kwaadwillige registratie van een domeinnaam en het hacken van een bestaande website. De URL helpt phishes te herkennen die op oude en waarschijnlijk gehackte domeinnamen zijn geplaatst.

Filters

Omdat alleen het absolute aantal van DNS-queries relevant is, worden de IP-adressen in de DNS-queries eruit gefilterd en niet verder verwerkt.
SIDN verwerkt de naam van de registrar, maar deelt met FHD alleen een pseudoniem daarvan. FHD verwijdert zo goed als mogelijk eventuele persoonsgegevens in URL's voordat FHD de URL met SIDN deelt.

Retentie

Domeinnamen die kwaadaardig gedrag tonen, slaan we voor onbepaalde tijd op. Daarmee is het in de toekomst mogelijk deze domeinnamen beter te onderzoeken en de detectie verder te verbeteren. In deze fase bevat de data geen persoonsgegevens meer.

Toegang

De informatie is toegankelijk voor het team van SIDN Labs en beheerders van SIDN en voldoet aan de ENTRADA toegangseisen die beschreven staan in de algemene ENTRADA-policy.

Publicatie/delen

SIDN deelt informatie met Fraudehelpdesk, een private Nederlandse stichting. Het gaat om de volgende data: Aantal queries per domeinnaam (maar niet de oorsprong van de query), registratiedatum, registrar-pseudoniem. Er is een Data Sharing Agreement met FHD.

Domeinnamen die met zeer hoge waarschijnlijkheid phishes zijn, en die nog niet van registrars, hosters of andere partijen verwijderd zijn, delen we via het Netcrafttool met betrokkenen partijen. We delen alleen domeinnamen die geen

	persoonsgegevens inhouden. Dit proces is onderdeel van de take down procedures van SIDN.
Type	Productie
Andere beveiligingsmaatregelen	Uitwisselen van informatie tussen SIDN en FHD gaat door een versleutelde verbinding en de verbinding is alleen toegankelijk voor deze twee partijen.