Privacypolicy

Just-In-Time Transmitted Exception Report (JITTER) pilot

Datum
04 januari 2021

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	Just-In-Time Transmitted Exception Report (JITTER) pilot
Ingangsdatum policy	4 januari 2021
Doel van de applicatie of het onderzoek	JITTER is een prototype dat o.b.v. machine learning waarschuwingen genereert voor domeinnamen die mogelijk gecompromitteerd zijn en waarop malafide content geplaatst kan zijn (bijvoorbeeld een phish). Hierdoor helpt JITTER bij het herkennen van misbruik voordat meldingen hiervan op abuse lijsten voorkomen. De JITTER-waarschuwingen komen tot stand op basis van afwijkend gedrag op DNS, infra en content niveau en hebben betrekking op second level domeinnamen. SIDN Labs kan deze waarschuwingen zelf niet goed evalueren en afhandelen, omdat hiervoor aanvullende informatie nodig is (bijvoorbeeld over veranderingen op URL-niveau). Realtime Register (RTR) heeft als registrar de mogelijkheid om JITTER-waarschuwingen beter te beoordelen, al dan niet via haar resellers of hosters. Gedurende een pilot zullen SIDN Labs en Realtime Register het JITTER-prototype daarom gezamenlijk evalueren.
Persoonsgegevens	Onderstaande gegevens worden door JITTER-verwerkt en bevatten mogelijk PII: **DRS (Domeinnaam Registratie Systeem)** ● Registratiedatum

- Domeinnaam
- Nameservers gekoppeld aan een domeinnaam

DMAP (Domain name Ecosystem Mapper)

- IP-adres waarop de website gekoppeld aan een domeinnaam wordt gehost (A/AAAA-record).
- Mailserver die gekoppeld is aan een domeinnaam (MX-record).

ENTRADA (ENhanced Top-level domain Resilience through Advanced Data Analysis)

- Domeinnaam

Feedy (aggregatie van abuse feeds)

- IP-adressen van webservers waarop in het verleden abusievelijke content werd gehost. Deze informatie wordt gebruikt als ground truth.
- URLs waarop abusievelijke content in het verleden abusievelijke content werd gehost. Deze informatie wordt gebruikt als ground truth.

Grondslag

JITTER helpt bij het proactief aanpakken van domeinnaammisbruik en draagt hierdoor bij aan een vellig .nl-domein.

Filters

JITTER gebruikt veelal geaggregeerde gegevens. Zo kijkt het systeem in het geval van ENTRADA naar netwerken (ASen) die domeinnamen hebben opgevraagd in plaats van unieke resolvers (IP-adressen).

Retentie

We bewaren de gegevens nog maximaal 2 jaar met als doel het evalueren en verbeteren van JITTER o.b.v. nieuwe trainingsvoorbeelden en het onderzoeken van de lange termijn impact.

Toegang

De data is alleen beschikbaar voor geautoriseerde gebruikers van SIDN Labs met een username/password. Gebruikers kunnen de machine waarop de data staat alleen vanaf het SIDN-netwerk bereiken middels SSH of via een systeem console.

Publicatie/delen

Worden er gegevens gedeeld met partijen 1) buiten SIDN?

Ja, waarschuwingen die JITTER genereerd worden gedeeld met Realtime Register. Hierdoor heeft Realtime Register de

mogelijkheid om domeinnaam-gerelateerd misbruik in haar portfolio nog beter aan te pakken.

Een waarschuwing bestaat uit een .nl-domeinnaam waarop afwijkend en potentieel verdacht gedrag is gedetecteerd, eventueel aangevuld een korte motivatie hoe de waarschuwing tot stand is gekomen.

Realtime Register deelt feedback over de kwaliteit en toegevoegde waarde van waarschuwingen met SIDN.

Zo ja, zijn de persoonsgegevens hier afdoende uit verwijderd? Zo niet, of als dat niet mogelijk is, is er met de partij waarmee gedeeld wordt een (verwerkers)overeenkomst getekend?

Er worden geen persoonsgegevens gedeeld. Een domeinnaam kan echter wel verwijzingen naar een natuurlijk persoon bevatten (zoals janjansen.nl).

Ook heeft Realtime Register als registrar de mogelijkheid om zelf de houdergegevens van een gedeelde domeinnaam op te zoeken.

SIDN en Realtime Register hebben een overeenkomst getekend waarin wordt ingegaan op de verwerking van persoonsgegevens.

2) Is de partij waarmee gedeeld wordt gevestigd buiten de EU? (zo ja, vraag de Privacy Board eventueel om advies)

Niet van toepassing.

Type	R&D Onderzoek
Andere beveiligingsmaatregelen	Niet van toepassing