Privacypolicy

MINIONS-SPIN

Datum
11 september 2019

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	MINIONS-SPIN
Ingangsdatum policy	09-09-2019
Doel van de applicatie of het onderzoek	Dit betreft een onderzoek waarbij twee projecten samenwerken: MINIONS (Mitigating IOT-Based DDoS Attacks via DNS) en SPIN (Security and Privacy for In-home Networks). Voor het MINIONS-NL project werken we samen met de TU Delft. De TU Delft beschikt met haar partners over een honeypot-netwerk waar IoT-apparaten in zitten. Deze IoT-apparaten zijn (mogelijk) kwetsbaar en worden direct aan het internet gehangen. Vervolgens wordt het dataverkeer van en naar deze apparaten gemeten. Binnen het SPIN project werken we aan methodes om thuisnetwerken die onveilige IoT-apparaten bevatten, veiliger te maken. Om methoden en technieken te ontwikkelen om onveilige IoT-apparaten te detecteren, moeten we eerst weten wat de karakteristieken van onveilige IoT-apparaten zijn. De data uit de IoT-honeypot biedt een blik op de aanvalspatronen die IoT-devices kunnen krijgen.
Persoonsgegevens	In het netwerkverkeer kunnen persoonsgegevens voorkomen. Specifiek zijn dit IP-adressen die (1) scannen om te kijken of het IoT-apparaat kwetsbaarheden bevat, of (2) commando's proberen uit te voeren op het apparaat, bijvoorbeeld om malware te installeren.

Daarnaast is het mogelijk dat wij IP-adressen van potentiele slachtoffers vastleggen: een aanvaller kan besluiten een DDoS aanval uit te voeren op een IP-adres van een natuurlijk persoon. Dit commando, inclusief IP-adres van het slachtoffer, zullen wij dan ook verwerken.

Het verwerken van deze persoonsgegevens is noodzakelijk voor het onderzoek, immers bevat de netwerkdata zoals aangeleverd IP-adressen, die wij dus vanaf het opslaan al verwerken. Daarnaast is het verwerken noodzakelijk om inzicht te krijgen in IoT-gedrag: waar komt de verspreiding van IoT-malware vandaan (bijv.: thuisverbinding of bedrijfsnetwerk, uit welk land of vanaf welke provider)?

Grondslag

Er is sprake van een gerechtvaardigd belang. Het verwerken van de persoonsgegevens is nodig om goed onderzoek te doen naar de veiligheid van IoT-apparaten, waarmee we methoden en technieken kunnen ontwikkelen die het internet veiliger maken.

Filters

Gedurende ons onderzoek zullen wij geen filters toepassen.

Retentie

De gegevens worden bewaard zolang het MINIONS-project actief is. Als het project niet verlengd wordt, zal MINIONS-NL eindigen op 1 mei 2020.

Toegang

Toegang tot de gegevens is voorbehouden aan:

- TU Delft MINIONS-medewerker: voor het opslaan van de data op onze server
- Het SIDN Labs SPIN-team
- Systeembeheerders van SIDN en SIDN Labs kunnen inloggen op het VMWare cluster en hebben (theoretisch) ook de mogelijkheid om zichzelf toegang tot de data te verschaffen.

De gegevens worden op een virtuele server bewaard, waarbij alleen bovengenoemde personen toegang hebben. Dit is door middel van logboeken achteraf te controleren.

Publicatie/delen

Nee, er worden geen ruwe gegevens gedeeld met andere partijen. Als er gepubliceerd wordt, zullen hierin geen persoonsgegevens genoemd worden.

Type

Onderzoek

Andere beveiligingsmaatregelen

De virtuele server staat in het netwerk van SIDN Labs en wordt afgeschermd door de SIDN Labs firewall, waardoor hij alleen toegankelijk is vanuit de server van de TU Delft, en ook vanuit het SIDN Labs netwerk. Toegang vanuit externe locaties is alleen mogelijk door in te loggen via de SIDN Labs VPN, alwaar authenticatie door middel van zowel een persoonlijk certificaat in combinatie met een gebruikersnaam en wachtwoord gebruikt wordt.

Gegevensuitwisseling tussen de TU Delft en SIDN Labs zal altijd versleuteld plaatsvinden, hetzij via SFTP, hetzij via een ander protocol over SSH.

De virtuele server wordt voorzien van het meest recente Ubuntu LTS-server besturingssysteem, waarbij automatische updates ingeschakeld is. Daarnaast wordt regulier handmatig op beschikbare updates gecontroleerd.