# Privacypolicy

BASTION


Datum
15 februari 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 | BASTION: firmware-BASed honeypoT Internet Of thiNgs |
| Ingangsdatum policy | 15 februari 2021 |
| Doel van de applicatie of het onderzoek | 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. Daaruit is het BASTION-project ontstaan als onderdeel van SPIN.<br><br>Binnen het MINIONS-NL-project hebben we ook met IoT-honeypots gewerkt (zie gerelateerde aanvraag MINIONS-SPIN, dd september 2019), echter bleek die data achteraf beperkt tot Mirai-gerelateerde botnets. Daarnaast hadden we alleen toegang tot de resultaten van analyses en niet in de ruwe netwerkdata.<br><br>Voor deze aanvraag willen we zelf honeypots gaan opzetten. In fase 1 gebruiken wij generieke honeypots, die wij specifiek inrichten op IoT-infecties. Bijvoorbeeld door het simuleren van CPU-architecturen die voor IoT-apparaten gebruikt worden, maar ook door specifieke poorten te openen (bijvoorbeeld Telnet op poort 23 om Mirai aanvallen te detecteren) of specifieke kwetsbaarheden beschikbaar te maken.<br><br>In fase 2 gebruiken we firmware bestanden van bestaande IoT-apparaten en draaien wij die gevirtualiseerd. In deze fase |

simuleren wij (kwetsbare) IoT-apparaten en meten wij hoe botnets deze apparaten aanvallen.

In beide fasen is het doel om geautomatiseerde aanvallen aan te trekken en te bepalen welke acties ondernomen worden en wat deze acties voor gevolgen hebben voor het netwerkverkeer van een apparaat. Deze datasets kunnen wij vervolgens gebruiken om de detectie van SPIN in te richten, alsmede om onze Machine Learning modellen te trainen in het herkennen van 'fout' netwerkverkeer.

## 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 potentiële 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)? Het netwerkverkeer dat verwerkt en opgeslagen wordt is geen gebruikersverkeer: het gaat om netwerkverkeer van malware.

## 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

Na een periode van 2 jaar worden de databestanden geanonimiseerd, hierbij worden persoonsgegevens (IP-adressen) uit de databestanden verwijderd. Databestanden waar anonimiseren niet mogelijk is, zullen worden verwijderd.

## Toegang

Toegang tot de gegevens is voorbehouden aan:

- Het SIDN Labs SPIN/BASTION-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

Wij zijn van plan om publicaties te gaan schrijven op basis van de data. De publicaties bevatten omschrijvingen van de data, waaronder analyses en (geanonimiseerde) voorbeelden.

De verzamelde (netwerkverkeers)data zal daarnaast op het SPIN IoT dataplatform gezet worden, waardoor de bijbehorende analyses publiekelijk beschikbaar worden. Hierbij wordt zorggedragen dat informatie die naar personen kan verwijzen, zoals IP-adressen, geanonimiseerd worden.

De verzamelde data wordt niet publiekelijk gedeeld, maar kan wel met onderzoeksinstellingen (universiteiten) gedeeld worden, zolang er een ‘data sharing’ overeenkomst aan ten grondslag ligt waarin wordt vastgelegd dat de in deze policy gestelde eisen aan correctheid, doelbinding, beveiliging, en publicatie, gewaarborgd worden.

## Type

R&D, 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 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.

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