Privacypolicy

Sinkhole

Datum
28 mei 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	Botnet-onderzoek
Ingangsdatum policy	28 mei 2021
Doel van de applicatie of het onderzoek	Het opzetten van een sinkhole met als doel het verzamelen van data over het gedrag van botnet clients. Botnets bestaan uit een verzameling van met malware geïnfecteerde computerapparatuur van thuisgebruikers en servers, zogenaamde botnet clients. Deze clients staan onder het beheer van de botnet herder. Deze herder kan een bot opdrachten geven. Deze opdrachten variëren van het verzamelen van privé gegevens (spionage) tot het meedoen aan een DDOS aanval (offensief gedrag) Deze activiteiten hebben een negatieve impact op zowel de eigenaar en/of gebruiker van de besmette client als het slachtoffer van een offensieve opdracht. Deze botnet clients maken gebruik van een centrale server (C&C) waarmee de herder opdrachten naar de bot kan versturen. De client zal periodiek contact opnemen met de server om nieuwe opdrachten te ontvangen of om gestolen gegevens te uploaden. Deze centrale server maakt gebruik van een domeinnaam, door analyse van de DNS query data is het soms mogelijk om een nog niet geregistreerde .nl domeinnaam te vinden, die gebruikt wordt door een botnet. SIDN Labs zal deze domeinnaam registreren en een sinkhole opzetten met als doel het monitoren

en loggen van de botnet clients die een connectie maken met deze server.

Ook eventuele resolver bugs die zorgen voor operationele problemen (en kwetsbaar zijn voor misbruik) kunnen op de bovenstaande manier worden geïdentificeerd.

Persoonsgegevens

Voor elke botnet client connectie wordt het volgende opgeslagen:

- Tijdstip
- Domeinnaam
- IP-adres
- Land (gekoppeld aan IP-adres)
- AS-nummer (gekoppeld aan IP-adres)

Grondslag

Het detecteren en opruimen van een botnet besmetting is in het belang van de eigenaar van de besmette computer. Deze eigenaar is het slachtoffer van mogelijke spionage malware en kan onvrijwillig worden ingezet bij DDOS aanvallen.

Er is ook een algemeen belang omdat botnets kunnen worden ingezet om servers op het internet onbereikbaar te maken d.m.v. een DDOS aanval.

Hierdoor hebben ook niet besmette Internetgebruikers last van botnet besmettingen.

De identificatie van resolver bugs zorgt voor het minimaliseren van het misbruik d.m.v. DDOS- aanvallen en draagt bij aan een veiliger internet.

Filters

Geen.

Retentie

De data zullen niet langer dan 18 maanden worden bewaard.

Deze periode is nodig omdat dan kan worden onderzocht of de besmetting afneemt en op welke manier deze afneemt. Er kan bijvoorbeeld een verschil zitten in afname per geografische locatie (Azie v.s. USA bijvoorbeeld)

Toegang

Alleen personeel van SIDN Labs heeft toegang tot de data d.m.v. sterke username/password combinaties of d.m.v. public/private keys. Het SIDN Labs personeel heeft een uitgebreide instructie over het belang van privacy gekregen.

Publicatie/delen	De gegevens worden niet in ruwe vorm gedeeld of gepubliceerd. Alleen geaggregeerde statistische gegevens worden gepubliceerd, op stats.sidnlabs.nl en in papers.
Type	R&D, onderzoek
Andere beveiligingsmaatregelen	Geen.