Privacypolicy

UvA malwaredetectie

Datum
11 december 2015

Classificatie
Publiek

Auteur
SIDN Labs

Blad
1/2

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	Onderzoek graph theory t.b.v. DNS malwaredetectie
Ingangsdatum policy	31-01-2016
Doel van de applicatie of het onderzoek	Botnets bestaan uit een verzameling van met malware geïnfecteerde computers van thuisgebruikers. Deze computers staan onder het beheer van de botnet-herder. Deze herder kan een bot opdrachten geven. Deze opdrachten variëren van het verzamelen van privégegevens (spionage) tot het meedoen aan een DDoS-aanval (offensief gedrag) Deze activiteiten hebben een negatieve impact op zowel de eigenaar/gebruiker van de besmette computer 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 bot zal periodiek contact opnemen met de server om nieuwe opdrachten te ontvangen of om gestolen gegevens te uploaden. De onderzoeker van de UvA zal pogen door middel van het gebruik van graph theory, nieuwe nog niet bekende malware domeinnamen te identificeren.
Persoonsgegevens	De oorspronkelijke dataset bevat IP-adressen van resolvers. Deze adressen worden door een medewerker van SIDN Labs geanonimiseerd voordat de dataset naar de onderzoeker gestuurd wordt. De data waar het onderzoek uiteindelijk mee plaats vindt bevat geen persoonsgegevens.

Grondslag	Het detecteren en opruimen van een malwarebesmetting is in het belang van de eigenaar van de besmette computer. Deze eigenaar is het slachtoffer van mogelijke spionagemalware 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 malwarebesmettingen.
Filters	De resolver IP-adressen worden geanonimiseerd d.m.v. een salted SHA-2 hash. De salt is geheim en wordt na het anonimiseren verwijderd.
Retentie	De data wordt voor de duur van het onderzoek (30 dagen) gebruikt en daarna verwijderd.
Toegang	Alleen personeel van SIDN Labs en de onderzoeker van de UvA hebben 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 gedeeld met de onderzoeker van de Universiteit van Amsterdam. Voor het onderzoek wordt een dag DNS-query data gedeeld met de onderzoeker. De volgende data-elementen worden gedeeld: • resolver IP-adres (geanonimiseerd) • .nl-nameserver IP-adres • domeinnaam • tijdstip Er is een data sharing overeenkomst tussen SIDN en de UvA afgesloten.
Type	Onderzoek
Andere beveiligingsmaatregelen	Data uitwisseling tussen SIDN en de UvA zal d.m.v. versleutelde e-mail/versleutelde download plaatsvinden.