Privacypolicy

Ransomware Deployment Analysis met Tesorion

Datum
15 juli 2019

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	Ransomware Deployment Analysis met Tesorion
Ingangsdatum policy	01-08-2019
Doel van de applicatie of het onderzoek	Het Nederlandse securitybedrijf Tesorion heeft op basis van binaire analyse het gedrag van een ransomware onderzocht. Deze ransomware stuurt na een infectie versleuteld informatie aan honderden domeinnamen. Een groot deel van de domeinnamen zijn legitiem en worden alleen gebruikt om de eigenlijke Command & Control Server te verbergen. Tussen de domeinnamen staan ook 60 .nl-domeinnamen. Tesorion en SIDN Labs doen nu samen onderzoek naar de verspreiding van deze ransomware op basis van query's die wij zien op onze name servers. Het doel is om te onderzoeken op welke landen de ransomware vooral gericht is, hoe de ransomware zich verspreidt en of de ransomware zich ook op Nederlandse partijen richt.
Persoonsgegevens	SIDN Labs deelt met Tesorion eenmalig alle query's vanaf begin 2019 die aan een van de 60 .nl-domeinnamen gericht is. De data bevat: - De volledige domeinnaam van de query - De query-ID van het DNS-pakket - De DNS-querytype - De Autonomous System Number van de resolver die de query verstuurt

- Het land van de resolver
- Een pseudoniem van de resolver IP

Alleen SIDN Labs beschikt over de mogelijkheid om het pseudoniem van de resolver te vertalen naar het echte IP-adres.

Grondslag

Deze analyse levert een bijdrage aan de veiligheid van het internet. We krijgen inzicht in de verspreiding van malware en kunnen een inschatting maken over het aantal geïnfecteerde machines. Bovendien krijgen we inzicht in de kwetsbaarheid van systemen in Nederland.

Filters

SIDN Labs deelt alleen query's met Tesorion die gericht zijn aan de verdachte domeinnamen en die dus relevant zijn voor het onderzoek. Omdat SIDN Labs alleen over querydata van 2 van 4 nameservers beschikt zijn de query's bovendien een sample van de volledige dataset.

Voordat SIDN Labs de query's deelt worden alle IP-adressen vervangen door een pseudoniem. Hiervoor gebruiken we de techniek "tokanization". Alleen SIDN Labs kan het pseudoniem vertalen naar de IP-adressen.

Retentie

De query's worden bij Tesorion alleen voor de periode van het onderzoek opgeslagen. Het onderzoek duurt tot 30.09.2019.

Toegang

Alleen Tesorion heeft toegang tot de query's. Alleen SIDN Labs weet van welke IP-adressen de query's gestuurd werden.

Publicatie/delen

Er worden geen persoonsgegevens gedeeld of gepubliceerd.

Type

Onderzoek

Andere beveiligingsmaatregelen

De query's worden beveiligd verstuurd via Cryptshare.