Privacy Policy

Ransomware Deployment Analysis with Tesorion

Date
15 July 2019

Classification
Public

Author
SIDN Labs

Page
1/2

Contact
T +31 26 352 5500
support@sidn.nl
www.sidn.nl

Office
Meander 501
6825 MD Arnhem
The Netherlands

Postal address
Postbus 5022
6802 EA Arnhem
The Netherlands

Title of application/study	Ransomware Deployment Analysis with Tesorion
Policy start date	01-08-2019
Purpose of application/study	Dutch security firm Tesorion has investigated the behaviour of a ransomware program by means of binary analysis. After infecting a machine, the ransomware in question sends encrypted information to hundreds of domain names. Many of the domain names in question are legitimate and addressed only to make identification of the true command and control server more difficult. The addressed domain names include sixty .nl domain names. Tesorion and SIDN Labs are now conducting a joint study of the distribution of the ransomware in question, which involves analysis of the query traffic handled by the .nl name servers. The purpose of the study is to identify the main countries targeted by the ransomware, and to clarify how the ransomware is spread and whether any of the targets are in the Netherlands.
Personal data	SIDN Labs will provide Tesorion with a single dataset covering all the queries sent to the sixty .nl domain names since the start of 2019. The shared data will consist of the following information about each query: - The full queried domain name - The query ID of the DNS packet - The DNS query type - The Autonomous System Number of the querying resolver

- The country where the resolver is based
- A pseudonym of the resolver IP

Only SIDN Labs will know the true IP address associated with each resolver pseudonym.

Legitimate basis	The analysis will contribute to internet security and stability. We will obtain insight into the distribution of malware and be able to estimate the number of infected machines. We will additionally obtain insight into the vulnerability of systems in the Netherlands.
Filters	The data shared with Tesorion will relate exclusively to suspect domain names; all the shared data will therefore be relevant to the research. Furthermore, because SIDN Labs has query data from only two of the four .nl name servers, the shared data will represent only a sample of the true full dataset. Before the data is shared, all IP addresses will be replaced by pseudonyms, using the 'tokenisation' technique. Only SIDN Labs will know the true IP address associated with each pseudonym.
Retention	The query data will be retained by Tesorion only for the duration of the research. The research is scheduled to run until 30.09.2019.
Access	Only Tesorion will have access to the shared query data. Only SIDN Labs will know the true IP addresses of the querying resolvers.
Publication/sharing	No personal data will be shared or published.
Type	Research
Other security measures	The query data will be transferred securely using via Cryptshare.