Oct 28 2023

NETMANAGEIT

Intelligence Report

PLAYCrypt Extortion Software Analysis

Table of contents

Overview

Entities

Observables

External References

Overview

Description

Analysis of PLAYCrypt, a ransomware tool developed by Balloonfly.

Confidence

This value represents the confidence in the correctness of the data contained within this report.

15 / 100

Content

N/A

Attack-Pattern

Name
T1192
ID
T1192
Name
Data Encrypted for Impact
ID
T1471
Description
An adversary may encrypt files stored on a mobile device to prevent the user from accessing them. This may be done in order to extract monetary compensation from a victim in exchange for decryption or a decryption key (ransomware) or to render data permanently inaccessible in cases where the key is not saved or transmitted.
Name
T1022

ID
T1022

Domain-Name

Value
mbrlkbtq5jonaqkurjwmxftytyn2ethqvbxfu4rgjbkkknndqwae6byd.onion
k7kg3jqxang3wh7hnmaiokchk7qoebupfgoik6rha6mjpzwupwtj25yd.onion

StixFile

Value
467772b65ad10a24a4749f53771cbb3f500636f4ca6d43f5bed894779ea72c09

External References

- https://otx.alienvault.com/pulse/653a76d73f6f320c3c91cb99
- https://www.antiy.cn/research/notice&report/research_report/PlayCrypt_Analysis.html