alien_technical_analysis_report.pdf

Sida 3 av 26

2

Introduction

Alien malware was first introduced in MaaS (Malware as a Service) forums by a user named ring0. The Alien pest appears to be an extension of Cerberus V1, according to ThreadFabric reports. It is estimated to have been developed by or separated from the Cerberus family as an alternative to the Cerberus pest, whose development was discontinued in early 2020. Cerberus malware, which did not offer a major innovation in May 2020, added the ability to steal information only from the Google Authenticator application, in addition to the previous version. The code structure that performs this malicious operation is almost identical to the Alien malware that was released in February 2020. This similarity raises suspicions that the developers of the Cerberus pest are related to the Alien developers.

Alien malware of Android Banking Trojan type is more capable than ordinary Banking Trojan malware. Alien malware has high-level capabilities such as transferring important information such as sms, contacts, call logs on the victim device to the remote server, executing commands from the C2 server, and reading incoming notifications.

Forum post