# AnubisBackdoor.md

github.com/prodaft/malware-ioc/blob/master/SavageLadybug/AnubisBackdoor.md

prodaft

prodaft/**malware-ioc**

This repository contains indicators of compromise (IOCs) of our various investigations.

7 Contributors | 0 Issues | 248 Stars | 24 Forks

## Anubis Backdoor

A Python-based backdoor used by the Savage Ladybug (FIN7) group is developed to provide remote access, execute commands, and steal data. It is obfuscated to avoid detection.

The full report is available here.

## Indicators of Compromise (IOC)

## Backend servers

```
38.134.148.20
5.252.177.249
212.224.107.203
195.133.67.35
```

## File Hashes

### SHA256

03a160127cce3a96bfa602456046cc443816af7179d771e300fec80c5ab9f00f

5203f2667ab71d154499906d24f27f94e3ebdca4bba7fe55fe490b336bad8919