Вирус может записывать нажатия клавиш, отправлять USSD-запросы, фиксировать активность на дисплее смартфона, перенаправлять звонки, а также собирать контакты и СМС; троян опасен функционалом автоматической блокировки и разблокировки устройства.

Троян маскируется под обновления Google Play, а для обмана пользователя применяется метод наложения окон. К тому же Antidot может активировать Virtual Network Computing (VNC), использовать функциональность расшаривания экрана смартфона, что даёт оператору зловреда удалённый доступ к гаджету.

При заражении смартфона троян запрашивает не только стандартные разрешения, но и системные — Accessibility Settings. Управляется вирус с сервера, с которого постоянно поступают команды. То есть злоумышленники могут следить за пользователем в режиме реального времени.