# How long does it take to get owned?

David Wardle

## Technical Report

RHUL–ISG–2019–4

27 March 2019


Information Security Group
Royal Holloway University of London
Egham, Surrey, TW20 0EX
United Kingdom

# Executive summary

This report investigates the use of stolen credentials; more specifically measuring the time it takes for them to be used after they have been leaked. By way of a literature review and technical research, it begins by looking at the concept of digital identity and the use of honeypots in information security. It then presents the different approaches and techniques that can be used to monitor access to an online account. It also describes the methods adopted by cybercriminals to illegally share personal data including passwords.

The report continues by presenting a framework that was designed to create fake online identities along with an infrastructure to monitor their activity. The design was implemented using a combination of manual processes and software developed for this project. The implementation was tested by publishing the credentials for eleven fake identities on paste websites. Over the course of six weeks, five events of unauthorised access were recorded, with the fastest occurring just 34 minutes after the leak.

The report concludes by discussing the results of the experiment, recommending improvements that can be made to the framework and proposing opportunities for future work.