Stolen online credentials: A hijacker's decision-making perspective

Renushka Madarie, Stijn Ruiter, Wouter Steenbeek, Edward Kleemans

Background/aim

As more and more data is being stored and transmitted, opportunities for data thieves increase considerably. Stolen personal data comes in many types. The present study revolves around the online dissemination of stolen credentials for online accounts. Leaked credentials enable potential account hijackers to hijack accounts without having to steal credentials themselves. By using an account hijacker's perspective, criminal decision-making theory is applied to study the choice alternatives and characteristics account hijackers face when searching online for stolen credentials. Two key phases in this process are discerned: searching for online platforms and searching for posts in which credentials are offered.

Method

Characteristics of three types of web platforms – cryptomarkets, web forums, and paste websites – along with relevant posts on these websites were analysed. The platforms were found by entering relatively simple search terms into well-known search engines. Platforms on which stolen credentials were leaked were collected from the first two results pages for each query. For each type of platform, the two platforms with most posts offering stolen credentials were selected for analysis.

Results/conclusion

The results of this study provide insight into the ways stolen credentials are disseminated online and how this differs for different types of platforms.