OskiStealerEN.pdf

Sida 3 av 18

Introduction

First thought to have surfaced in November 2019, the "Oski Stealer" malware showcases its ability to steal sensitive information, credentials and data from cryptocurrency wallets from more than 60 apps. The name Oski is derived from an old Norse word meaning "Viking Warrior". The malware targets the following data;

Login information in apps

Browser information (cookies, autofill, credit card information)

Screenshots

System information

Cryptocurrency wallets (Bitcoin, Ethereum, Litecoin etc.)

The oski pest, which is offered for sale on Russian underground platforms and has an easy interface, is offered for sale at a price between $ 70 and $ 100. It is a family of malware that is highly preferred by hackers because it is affordable and steals a lot of data. Customers on underground forums by contacting Oski Stealer developers buys malware and develops it and distributes it to its targets. The malware family, which has a great reputation on the underground forums, receives a lot of positive feedback from its customers, which can be cited as an indication of how stable the oski malware is.

Although Oski is mostly seen in North America, it has recently started to be seen in China as well. As with many malware, Oski malware It aims to spread using the phishing technique.

First Look

Oski malware downloads 7 DLLs from the C&C server and uses these DLLs to steal the data it targets. It was observed that the anti-debug method used by Oski Stealer malware was incomplete in preventing dynamic analysis. It only checks the system name as an anti-debugging technique.

The information the malware collects Under C:\ProgramData folder saves in a file of random characters then this file makes a zip file and creates an http post request and sends this file to the C&C server in an encrypted way.

3
