Brief technical analysis of the "Poseidon Stealer" malware

By Federal Department of Defence, Civil Protection and Sport DDPS

Archived: 2026-04-05 17:06:26 UTC

Brief technical analysis of the "Poseidon Stealer" malware

11.07.2024 - At the end of June 2024, cybercriminals spread the malware "Poseidon Stealer" in German-speaking Switzerland by email, using AGOV as a lure with the aim of infecting computers with the macOS operating system. The NCSC has now produced and published a brief technical analysis of the malware.

At the end of June, the NCSC received numerous reports on emails that pretend to come from AGOV, the Swiss government login. The malicious emails asked the recipients to download a software package for macOS, which in fact was a malware called "Poseidon Stealer".

The brief technical analysis by NCSC shows how "Poseidon Stealer" works in order to access and steal the victims' data. It has been shown that once the malware has been installed, it searches the computer for and collects sensitive information such as login data, private keys, cookies and crypto wallets. This data is then compressed into a zip file and sent to a central botnet command and control server. One thing to emphasize about this malware is that as soon as the data has been drained and after the infected device is restarted, it remains on the device but is no longer executed.

NCSC notification dated June 28, 2024
