27. Juli 2020 Studie · Web & Cloud · Mobile Sicherheit

Analyse des Electroneum Cloud Miners

Der Volltext liegt derzeit nur in der Fassung „English“ vor. Die Übersetzung folgt.

Archiviert. Dieser Inhalt wird nicht mehr aktualisiert. Er bleibt zur Information verfügbar.

Quelle https://technology2.a-sit.at/veroeffentlichungen/analyse-des-electroneum-cloud-miners/

Bei Electroneum handelt es sich um eine der ersten Kryptowährungen, die “Mobile Mining” unterstützt. Dabei wird den Nutzern der App für die Benutzung regelmässig eine Belohnung ausgeschüttet. Dafür muss ein Electroneum Account angelegt und aktiviert, sowie der “Cloud Mining” Prozess gestartet werden. Für die Aktivierung des “Cloud Mining” Prozesses müssen zwei Selfies in einer vorgegebenen Pose oder mit einer vorgegebenen Zeichnung erstellt werden. In diesem Projekt analysieren wir die Sicherheitsmechanismen und zeigen wie sie umgangen werden können. Beispielsweise verwenden wir AI-generierte Bilder um den Selfie-Check zu umgehen. Wir zeigen wie ein Angreifer einen Bot erstellen und betreiben könnte, der mehrere Accounts simuliert und dadruch einen größeren Teil der Belohung abräumen könnte. Das Electroneum-Team wurde über diese Schwachstelle im Rahmen eines „Responsible Disclosure“ Prozesses informiert. Nach der Meldung der Lücke, wurde Cloud Mining eingestellt. Daher kann der beschriebene Angriff nicht mehr durchgeführt werden.