Neue Android-Ransomware tarnt sich als Covid-19-App - ESET stellt kostenloses Entschlüsselungs-Tool bereit

Die Experten des IT-Sicherheits-Herstellers ESET warnen davor, Corona-Warn-Apps ohne genaue Überprüfung zu installieren. Im aktuellen Fall entdeckten die Security-Forscher eine Android-Ransomware, die sich als kanadische Covid-19-App tarnt. Diese verschlüsselt nach der Installation das Android-Gerät und fordert ein Lösegeld. Die Hintermänner des als "CryCryptor" getauften Verschlüsselungstrojaners machten sich die Ankündigung der kanadischen Regierung zunutze, eine offizielle App zur Kontaktverfolgung zu unterstützen.
"Es ist klar, dass die Operation mit CryCryptor so konzipiert wurde, dass sie sich an die offizielle COVID-19-Tracing-App anlehnt", kommentiert Lukas Stefanko, der die ESET-Untersuchung leitete. Mithilfe zweier COVID-19-Themen-Websites lockten die Angreifer ihre Opfer zum Herunterladen eines vermeintlich offiziellen COVID-19-Tracing-Tools. Dahinter verbirgt sich jedoch eine getarnte Lösegeld-App. Dank eines Tweets, der die Entdeckung einer gefälschten Android-Banking-Malware ankündigte, kam er mit seinem Forscher-Team diese Lösegeldoperation auf die Schliche.

"Neben der Verwendung einer hochwertigen mobilen Sicherheitslösung raten wir Android-Benutzern, nur Anwendungen aus seriösen Quellen wie dem Google Play-Store zu installieren", sagt Stefanko von ESET. Beide Websites sind mittlerweile außer Betrieb.

Kostenlose Entschlüsselung möglich

Opfer von CyrCryptor haben Glück im Unglück. ESET-Forscher entwarfen umgehend ein Entschlüsselungstool, das unter https://github.com/eset/cry-decryptor heruntergeladen werden kann. "CryCryptor enthält einen Fehler in seinem Code. Dieser erlaubt jeder Anwendung, die auf dem betroffenen Gerät installiert ist, einen beliebigen Dienst zu starten, der von der fehlerhaften Anwendung bereitgestellt wird. Also haben wir ein Tool erstellt, das die in CryCryptor eingebaute Entschlüsselungsfunktionalität startet", erklärt Lukás Stefanko.

Eine detaillierte Analyse von CryCryptor ist auf dem ESET-Security-Blog veröffentlicht: