mVISE
MOBILITY - VIRTUALIZATION - SECURITY

*„TURNING OFF YOUR PHONE IS MEANINGLESS, ALL YOUR DATA IS ALREADY STORED ON OUR SERVERS! WE STILL CAN SELLING IT FOR SPAM, FAKE, BANK CRIME etc...“*

(Zitat der Batterie Sparer App „Energy Rescue“, strings.xml:95)

# mVISE schaut hin: Energy Rescue

Im Rahmen der Fokussierung von mVISE auf Security-Themen haben sich unsere Mobile Security Experten die Android Malware „Energy Rescue” im Detail angesehen. Wir konnten neben den aus der Presse bekannten Informationen weitere interessante Details herausfinden.

## Worum geht es?

Ende November 2016 wurde in den offiziellen Google Play Store eine App zum kostenlosen Download eingestellt, die dem Benutzer versprach, die Akkuleistung seines Smartphones zu verbessern. Ein Versprechen, das sicherlich attraktiv für jeden Intensiv-Nutzer ist. Jedoch läutete die App mit dem wohlklingenden Namen „Energy Rescue“ die nächste Stufe in der Entwicklung von Malware auf mobilen Devices ein.

Die Malware wurde von unserem Partner Check Point aufgedeckt und der „Charger Ransomware“ Familie zugeordnet[1]. Check Point ist ein Anbieter, der mit seiner Mobile Security Lösung „Check Point Mobile Threat Prevention“ (MTP), Schutz gegen Ransomware der Familie „Charger“ bietet. MTP untersucht nicht nur alle installierten Applikationen auf einem mobilen Gerät, sondern auch das darunterliegende OS und spürt sogenannte Man-in-the-Middle (MitM) Angriffe auf.

**Berechtigungen:**

- Zustand und Identität des Smartphones auszulesen (Handynummer, Seriennummer, usw.)
- SMS oder MMS auszulesen
- Kontaktdaten abgreifen
- Schreiben auf der SD-Karte
- Profile des Nutzers auszulesen
- Voller Internetzugang verschaffen

**UNSER TIP:** Berechtigungen immer kritisch hinterfragen!

## Was macht „Energy Rescue“ im Detail?

Die Android Applikation „Energy Rescue“ liest neben den gespeicherten SMS alle Kontakte auf dem mobilen Device aus und erfragt für die Durchführung einer Optimierung nach administrativen Rechten. Willigt der Benutzer ein, so wird das mobile Device gesperrt und der Nutzer erhält eine eindeutige Erpressungsnachricht. Darin wird der Benutzer aufgefordert 0,2 Bitcoins (ca. 170€) zu zahlen, um das Telefon zu entsperren und den Weiterverkauf potenzieller gekaperter Daten zu verhindern. „Freundlicherweise“ unterstützt die App auch direkt den Einkauf von Bitcoins (siehe unten).

Technische Details: Bislang kannte man vor allem das Phänomen, dass Ransomware den bösartigen Schadcode in der Regel nach der ersten Ausführung nachlädt. „Energy Rescue“ hingegen beinhaltet einen Schadcode, der bereits verschlüsselt in der App mit ausgeliefert wird.

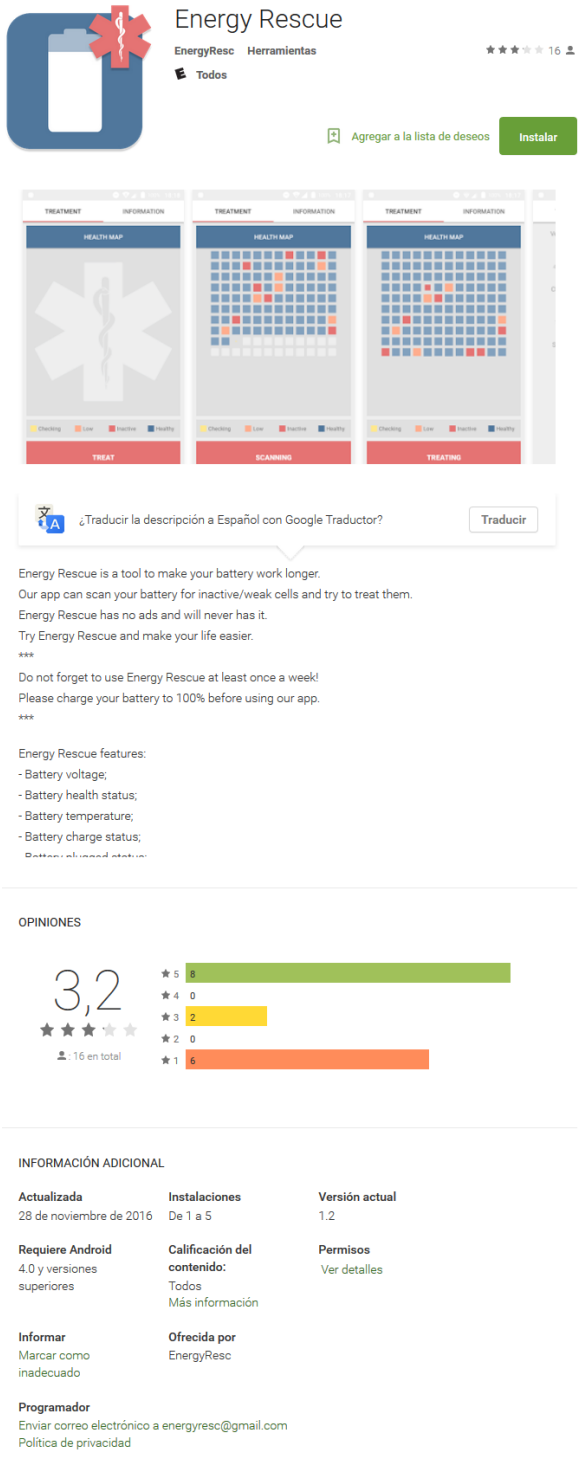
Weiterhin hat die App mehrere Mechanismen, um eine dynamische Codeanalyse zu erkennen. Diese Mechanismen sind allerdings in einigen Ländern (Ukraine, Russland und Weißrussland) nicht scharf geschaltet.

Wir haben direkt bei Vivien Raoul, CTO & Co-Founder der aus Frankreich stammenden Security Software „Pradeo“[2] nachgefragt. Laut seiner Aussage ist dieses Verhalten „ziemlich ungewöhnlich und

[1] http://blog.checkpoint.com/2017/01/24/charger-malware/

[2] https://www.pradeo.com/en-US/

stellt das vollautomatisierte Testen von Applikationen vor neue Herausforderungen“. Pradeos „Pradeo Apps Security“ bietet eine Lösung zum automatisierenden Bewerten von mobilen Applikationen aus IT Security Sicht, mit der neben unsauberen Implementierungen auch offensichtliche Informationsströme und Sicherheitslücken erkannt werden können.




## Was haben wir herausgefunden?

Zwar ist es eine Unart vieler mobile Applikationen nach vielen Rechten zu verlangen, allerdings könnte ein aufmerksamer Nutzer alleine dadurch an der Intention der App – das Verbessern der Akkulaufzeit – zweifeln.

Bei unserer statischen Codeanalyse sind wir auf eine Datei gestoßen, die unter anderem URLs zu legitimen Bitcoin-Verkäufern auflistete.

Die Liste beinhaltet diverse Seiten, die sich mit dem Verkauf von Bitcoins beschäftigen. Spätestens hier kommen starke Zweifel auf, dass die App der Verlängerung der Akkulaufzeit dient.

Weitere Analysen haben unter anderem folgende Textfragmente gezeigt, die wir zur einfachen Lesbarkeit neu sortiert haben.

„TURNING OFF YOUR PHONE IS MEANINGLESS, ALL YOUR DATA IS ALREADY STORED ON OUR SERVERS! WE STILL CAN SELLING IT FOR SPAM, FAKE, BANK CRIME etc...“

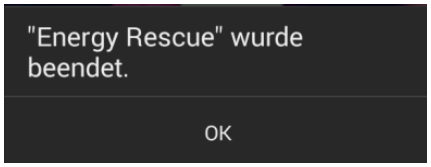
Und weiter wird erklärt:

1. You need to register Bitcoin Wallet (FREE) - https://blockchain.info/wallet/
2. Buying Bitcoin is easy, you can ask your friends or use any official exchanges guides:
BTC to Bitcoin address:

- https://Paxful.com
- https://CoinJar.com
- https://LocalBitcoins.com
- https://Coinbase.com
- https://Bitstamp.net
- https://Bitquick.com
- https://Coincorner.com

4. In the description of the payment enter the unique KEY by which we could identify your device.
5. Wait until we approve your payment and Unlock your mobile device. It may take a couple of hours.

Bei unserer dynamischen Codeanalyse ist aufgefallen, dass die Malware die Ausführung in einer virtuellen Umgebung erkennt und sich als Gegenmaßname selbstständig beendet.




Zu guter Letzt haben wir uns das Zertifikat angesehen, mit der die App signiert wurde. Das Zertifikat ist aus rein technischer Sicht einwandfrei. Jedoch lässt sich, wie die untenstehende Tabelle zeigt, der Urheber der App nicht aus dem Zertifikat identifizieren. Dies ist ein deutliches Zeichen dafür, dass es sich auf keinen Fall um eine vertrauenswürdige Applikation handelt.

| | ENERGY RESCUE | SALESPHERE |
|---|---|---|
| CN: | dfsdfds435 | SaleSphere |
| OU: | fsdf5345345 | SaleSphere Releases |
| O: | 45rwe | mVISE AG |
| L: | sdfwefewrewr | Duesseldorf |
| ST: | we | North Rhine-Westphalia |
| C: | 4tert | DE |

Im direkten Vergleich zu einer legitimen App wie unserer eigenen SaleSphere[3] ist leicht zu erkennen, dass es sich bei dem Zertifikat von „Energy Rescue“ um eine Fälschung handelt. Das hätte den Automatismen bei Google auffallen müssen.

**Über den Autor**

**Bernhard Borsch** ist seit zwei Jahren als Senior Consultant im Bereich Security für die mVISE AG tätig. Zu seinen Kernkompetenzen zählt neben PKI und Kryptographie auch das Themenfeld Mobile Security.

Zurzeit unterstützt er mit seinem Team Kunden, die sich der Herausforderung der Absicherung von mobilen Devices stellen. Professionelle und fachkompetente Beratung sind sein Schlüssel zum Erfolg.

## Was bietet mVISE an?

Diese Art von Bedrohung beweist, dass ein statisches Regelwerk – wie es ein MDM oder EMM bietet – nicht ausreicht, um sich zu schützen. Unsere Experten haben ein eigenes Programm zusammengestellt, um unseren Kunden zu ermöglichen, sich mit geeigneten Maßnahmen gegen Bedrohungen dieser Art auf ihren mobilen Devices zu schützen. Unsere Experten bieten Workshops zu Themen wie Applikationssicherheit, dynamischer und statischer Codeanalyse und Mobile Threat Protection.

Das Sensibilisieren von Mitarbeitern ist ein erster Schritt hin zu einem sicheren Einsatz von mobilen Devices im Unternehmen – jedoch nur der erste von mehreren.

Bernhard Borsch

Senior Security Consultant bei der mVISE AG
Mail: bernhard.borsch@mvise.de
Mobil: +49 152 34151236

[3] https://www.salesphere.de