Analyse der Ransomware „Energy Rescue“

Schadsoftware auf mobilen Android-Geräten lockt Nutzer in die Bitcoin-Falle. mVISE IT-Security-Experten nehmen die Ransomware *„Energy Rescue“* ins Visier. Erfahren auch Sie, wie Sie sich vor möglichen Schadsoftware-Angriffen schützen können.

Zusammenfasung

Ende November 2016 wurde im offiziellen GooglePlay Store eine kostenlose App bereitgestellt, die Benutzern versprach, die Akkuleistung ihrer Smartphones zu verbessern. Ein Versprechen, welches für eine Vielzahl an Nutzern attraktiv erschien und so unzählige Geräte infizieren konnte. Unter dem Namen *„Energy Rescue“* wurde so die nächste Stufe in der Entwicklung von Malware auf mobilen Devices eingeläutet.

Aufgedeckt wurde die Ransomware von unserem Partner Check Point. Check Point ist ein Anbieter, der mit seiner Mobile-Security-Lösung *„Mobile Threat Prevention“* (MTP), Schutz gegen Ransomware der Familie *„Charger“* bietet. Auch *„Energy Rescue“* lässt sich genau dieser *„Charger Ransomware“*-Familie zuordnen.

Durch MTP werden nicht nur alle installierten Applikationen auf einem mobilen Gerät untersucht, sondern auch das darunterliegende Betriebssystem. Dadurch können sogenannte *„Man-in-the-Middle“*(MitM)-Angriffe aufgespürt werden.

Im Folgenden betrachten wir die Herangehensweise der Ransomware genauer und weisen auf die Notwendigkeit einer ausreichenden Sensibilisierung aller Mitarbeiter hin.

Funktionsweise „Energy Rescue“

Die Android-Applikation *„Energy Rescue“* liest, neben den gespeicherten SMS, alle Kontakte auf dem mobilen Gerät aus und erfragt, für die weitere Nutzung und die Durchführung einer Optimierung, administrative Rechte. Willigt der Benutzer ein, so wird das mobile Device gesperrt und dem Nutzer wird eine eindeutige Erpressungsnachricht angezeigt. Darin wird er aufgefordert 0,2 Bitcoins (ca. 170€) zu zahlen, um das Gerät zu entsperren und den Weiterverkauf seiner potenziell gekaperten Daten zu verhindern. Im Zuge dieser Erpressung wird – „freundlicherweise“ – der direkte Einkauf von Bitcoins unterstützt (siehe unten).

TECHNISCHE DETAILS

Bislang war es für Ransomware üblich, den bösartigen Schadcode in Folge der ersten Programmausführung nachzuladen. *„Energy Rescue“* hingegen beinhaltet einen Schadcode, der bereits verschlüsselt während des Downloads enthalten ist. Darüber hinaus hat die App interne Mechanismen, eine dynamische Codeanalyse erkennen zu lassen. Diese Mechanismen sind allerdings in einigen Ländern (vgl. Ukraine, Russland und Weißrussland) deaktiviert. Auf unsere Anfrage bei dem französischen Security-Softwareentwickler *Pradeo*, antwortete CTO & Co-Founder, Vivien Raoul: *„Dieses Verhalten sei ziemlich ungewöhnlich und stellt das vollautomatisierte Testen von Applikationen vor neue Herausforderungen“*.

Pradeos „Apps Security“ bietet eine Lösung zur automatischen Bewertung von mobilen Applikationen aus IT-Security-Sicht, mit der, neben unsauberen Implementierungen, auch offensichtliche Informationsströme und Sicherheitslücken erkannt werden können.

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

Ergebnisse

Zwar ist es eine Unart mobiler Applikationen nach umfangreichen Rechten zu verlangen, allerdings könnte ein aufmerksamer Nutzer allein dadurch an der Intention der App – dem Verbessern der Akkulaufzeit – zweifeln.

Durch unsere **STATISCHE CODEANALYSE** sind wir auf eine Datei aufmerksam geworden, die unter anderem URLs zu legitimen Bitcoin-Verkäufern auflistet. Diese Liste beinhaltet diverse Seiten, die sich mit dem Verkauf von Bitcoins beschäftigen. Spätestens hier kommen starke Zweifel auf, dass *„Energy Rescue“* der Verlängerung der Akkulaufzeit diene.

Weitere Analysen haben unter anderem folgende Textfragmente gezeigt, die wir zur erleichterten 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 OR CRIME … ”

Und weiter wird angewiesen:

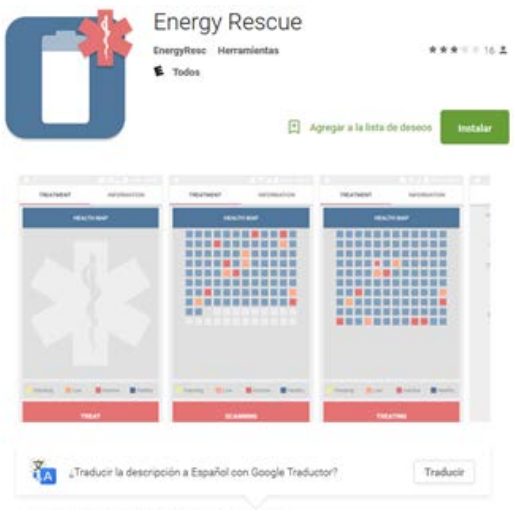
1. You need to register Bitcoin Wallet (FREE)
   - https://blockchain.info/wallet/
2. Buying Bitcoin is easy, you can ask your friends or use any official exchanges guides:
   BTC to Bitcoin address:
   - https://Paxful.com
   - https://CoinJar.com
   - https://LocalBitcoins.com
   - https://Coinbase.com
   - https://Bitstamp.net
   - https://Bitquick.com
   - https://Coincorner.com
3. In the description of the payment enter the unique KEY by which we could identify your device.
4. 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 Gegenmaßnahme selbstständig beendet.

Abschließend haben wir das Zertifikat, mit welchem die App signiert wurde, betrachtet. Dieses ist, aus rein technischer Sicht, einwandfrei. Jedoch lässt sich, wie die untenstehende Tabelle zeigt, der Urheber der Anwendung nicht identifizieren. Dies ist ein deutliches Zeichen dafür, dass es sich um eine nicht-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 die mVISE SaleSphere-Applikation[2], ist leicht zu erkennen, dass es sich bei dem Zertifikat von *„Energy Rescue“* um eine Fälschung handelt. Es ist nicht zu bestreiten, dass diese Auffälligkeit den Automatismen des Google Play Store hätte auffallen müssen.



[2] https://www.salesphere.com

Profitieren Sie von qualifizierten Lösungen

Der Befall einer Schadsoftware zeigt, wie sensibel der Umgang mit vertraulichen Daten ist. Diese Art der Bedrohung beweist, dass ein statisches Regelwerk – wie es ein MDM (Mobile Device Management) oder EMM (Enterprise Mobility Management) bietet – nicht ausreicht, um vertrauliche Daten zu schützen.

Wir haben ein eigenes Programm zusammengestellt, das unseren Kunden ermöglicht, sich mit geeigneten Maßnahmen gegen Bedrohungen dieser Art zu schützen. Unsere Experten bieten Workshops zu Themen wie Applikationssicherheit, dynamischer und statischer Codeanalyse und Mobile Threat Protection an.

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

Wir begleiten Sie auf Ihrem Weg
in eine sichere Zukunft – sprechen Sie uns an!

ÜBER DEN AUTOR

Bernhard Borsch ist seit 2014 für die mVISE AG tätig. Als Manager für das IT-Security Consulting beraten sein Team und er Kunden zum Thema IT-Security im Zuge der Herausforderungen der Digitalisierung. Zu seinen persönlichen Themenfeldern gehört neben den klassischen Themen, wie Enterprise- & Cloud-Security, PKI und Kryptographie, auch Zukunftsthemen der IT-Security, wie Blockchain und Deception Technology. Professionelle und fachkompetente Beratung sind sein Schlüssel zum Erfolg.

mVISE

Wir unterstützen mittelständische und große Unternehmen aller Branchen dabei, von der digitalen Revolution zu profitieren. Die besondere Kombination aus firmeneigenen Software-Lösungen mit ausgewählten Experten-Teams in den relevanten und aktuellen IT-Themengebieten schafft nachhaltige Wettbewerbsvorteile für unsere Kunden.

Unsere Experten bestimmen, gestalten, kreieren und steuern IT-Infrastrukturen und Software-Lösungen für Datenintegrations- und Enterprise-Data-Management-Projekte, mit dem Ziel, die aktuellen Geschäftsmodelle unserer Kunden zukunftssicher zu machen und gleichzeitig neue Geschäftsmodelle zu identifizieren.

Sprechen Sie uns an – gerne stellen wir Ihnen unser Angebot
in einem persönlichen Gespräch näher vor.
service@mvise.de | www.mvise.de

mVISE AG
Wahler Straße 2
40472 Düsseldorf
Fon: +49 211 78 17 80 – 0