Die Digitalbotschafter informieren!

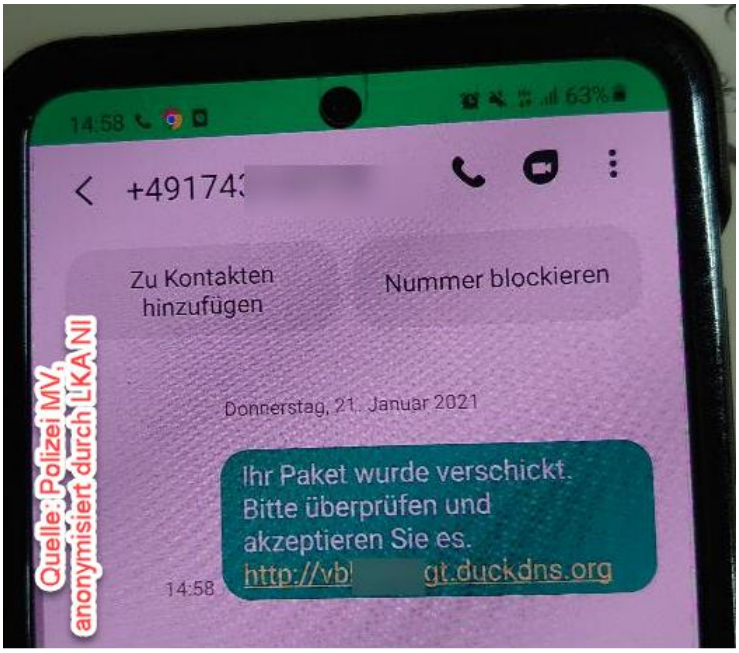
Heute das Thema: Abzocke mit SMS

Paketbenachrichtigungslink verursacht massenhafte SMS

Wie das Bundeskriminalamt und einige Landeskriminalämter, auch das LKA Rheinland-Pfalz mitteilt, gibt es Hinweise auf eine neue/ungewöhnliche Masche. Mehrere Smartphone-Nutzer bekamen eine SMS mit einem Link. Der Inhalt der Nachricht war:

„Ihr Paket wurde verschickt. Bitte überprüfen und akzeptieren Sie es. http://v…..jxgt.duckdns.org“

(Link durch uns gekürzt, siehe auch Bild)



Vorsicht vor Endung "duckdns.org"

Personen, die auf den Link geklickt haben, berichten, dass eine Software nachgeladen wurde und kurz danach über den Tag verteilt mehrere hunderte SMS von verschiedenen Rufnummern zugestellt wurden, die alle die gleiche Nachricht enthielten. Möglicherweise werden andere Links gezeigt, die jedoch bisher alle auf **duckdns.org** endeten.

Diese Nachricht stammt von keinem echten Transportdienstleister. Die Täter nutzen scheinbar derzeit die Corona-Pandemie aus, in der viel online bestellt wird. So ist es sehr wahrscheinlich, auf Personen zu treffen, die einer solchen SMS glauben, da Sie selbst Pakete erwarten.

Bei dem Anhang handelt es sich um Schadsoftware, die unter anderem SMS und MMS senden/empfangen kann, sowie eine Fernsteuerung des Smartphones zulässt. Diese Schadsoftware leitet unbemerkt sensible Daten weiter, spioniert die Kontaktliste der Geschädigten aus und versendet anschließend eigenständig SMS

mit der Schadsoftware an verschiedene Rufnummern, die zusätzliche Kosten verursachen können.

In einem Fall wurden über das Smartphone einer Frau **aus Mainz rund 1000 solcher SMS** an ihre Kontakte versendet, wodurch ein Schaden in dreistelliger Höhe entstand.

Maßnahmen, die Sie machen können, wenn Sie eine solche SMS bekommen haben:

- Klicken Sie auf keinen Fall auf Links, die Ihnen von unbekannter Seite und unerwartet zugestellt werden. Sollten Sie den Absender tatsächlich kennen, fragen Sie nach, was sich hinter dem Link verbirgt und ob der Versand beabsichtigt war.
- Bestätigen Sie keine Installation von fremden Apps auf Ihrem Smartphone. Besonders Android-Geräte sind hier gefährdet, da diese bei ungünstiger Einstellung eine Fremdinstallation und somit auch schädliche Apps zulassen.
- Deaktivieren Sie bei Android die Möglichkeit, unbekannte Apps installieren zu können. Möglicherweise ist in Ihrer Android-Version diese Funktion nicht mehr im Sicherheitsbereich zu finden. Geben Sie unter Einstellungen in der Suche „**unbek**“ an. Eventuell werden Sie nun in den Bereich „Unbekannte Apps installieren“ geführt, bei denen Sie einzelnen Apps diese Erlaubnis erteilen oder noch besser entziehen können. Ohne diese Erlaubnis können keine fremden Apps (also alles außerhalb des originalen App-Stores) installiert werden. Je nach Android und Smartphone kann diese Einstellung anders sein.
- Richten Sie unbedingt bei Ihrem Mobilfunkprovider die Drittanbietersperre ein, um weitere Kosten zu vermeiden. Diese kann kostenlos über den jeweiligen Service gebucht werden.
- iOS Nutzer dürften mit dieser SMS keine Probleme bekommen, da Apps nicht einfach so installiert werden können. Dennoch raten wir von einem Anklicken des Links ab.
- Wenn Sie eine oder ein paar wenige SMS (wie oben dargestellt) bekommen haben, dann muss es nicht bedeuten, dass Sie bereits die Schadsoftware installiert haben. Die Täter versuchen durch diese SMS ihre Schadsoftware, u.a. auch über die bereits infizierten Smartphones anderer Personen weiterzuverbreiten.
- Solange Sie unter Android den Link nicht angeklickt haben und die App installiert haben, ist Ihnen noch nichts passiert. Wichtig dabei ist, dass Sie die Installation von unbekannten Apps deaktiviert haben (siehe weiter oben).

Wenn Sie bereits geklickt, installiert und die SMS nun massenhaft bekommen und/oder selber versenden

Die Digitalbotschafter informieren!

- Schalten Sie Ihr Smartphone in den Flugmodus.
- Informieren Sie Ihren Provider
- Richten Sie, wenn nicht bereits geschehen, die Drittanbietersperre ein
- Prüfen Sie, ob durch die SMS bereits Kosten zu Ihrem Nachteil verursacht wurden. Ggf. können Sie einen Kostennachweis bereits beim Provider einholen/erfragen.
- **Erstatten Sie Anzeige bei Ihrer örtlichen Polizeidienststelle.** Bringen Sie dazu das Smartphone, Ggf. Screenshots/Abfotografieren mit einem anderen Smartphone, Kostennachweise usw. mit.
- Im schlimmsten Fall hilft nur die Zurücksetzung in den Auslieferungszustand.

Sie haben Fragen zu diesem und anderen Themen rund um Smartphone und Computer! Bitte wenden Sie sich per E-Mail oder Telefon an

Hans-Peter Demsar, E-Mail digibo.demsar@pdemsar.de, Tel: 0179 2380744 oder einen anderen der DiBo/-innen auf dieser Internet-Seite.