Shared content spoofing based on OG (Open Graph) protocol forgery

Description

Apple's Messages app supports the parsing of shared links and displays them in the form of title and image, allowing users to get a preview of the content (shown in Figure 1).

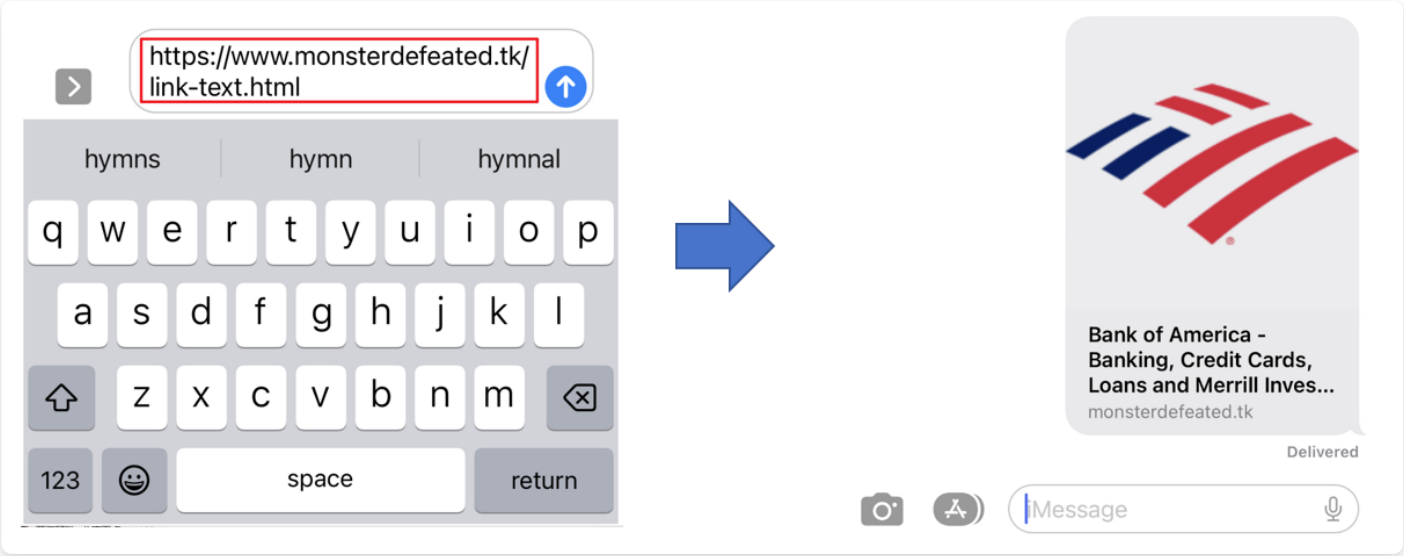

Figure 1: shared content preview based on OG protocol

However, this preview scheme can lead to phishing attacks. Since Apple's Messages app utilizes the OG (Open Graph) protocol for link previews, attackers can deceive the message receivers by disguising the phishing web pages using the OG protocol (shown in Figure 2).
In this way, the phishing page will be previewed as a harmless and trustworthy shared content as shown in Figure 1.

Figure 2: forge the OG protocol attributes in the phishing page

How to reproduce

We need a pre-made phishing page, and then we only need to add the following fields to the header of the page.

```
<head>
        <meta property="og:title" content="XXX" />
        <meta property="og:description" content="XXX" />
        <meta property="og:type" content="XXX" />
        <meta property="og:image" content="XXX" />
        <meta property="og:url" content="XXX" />
        <meta property="og:site_name" content="XXX" />
</head>
```