Investigating a Fake KDDI Smishing Campaign that abuses Duck DNS

systemweakness.com/investigating-a-fake-mobile-payment-smishing-that-abuses-duck-dns-d07c72468ba8

Lena June 23, 2023

【利用停止予告】KDDI未払い料金お支払いのお願い。http://lhuyykzzlv.duckdns.org

Recently in Japan, there has been an increase in Smishing attacks that abuse Duck DNS. In this blog post, I will be investigating one of these Duck DNS smishing attacks. The one analyzed here impersonates a mobile payment system.

Table of contents

The SMS message

The message says,

> 【利用停止予告】KDDI未払い料金お支払いのお願い。http://lhuyykzzlv[.]duckdns.org

Which translates to,

> [Suspension Notice] Please pay the unpaid KDDI fees. http://lhuyykzzlv[.]duckdns.org

Upon access, it leads to a blank page. Inspecting the element will show that it leads to another DuckDNS page.

This page has an IP of 45.12.138[.]87.

According to VirusTotal's Passive DNS Replication, it has many other Duck DNS domains associated with it.

It then led me to another Duck DNS page. Inspecting the page showed that the next redirect will differ based on the User Agent. For an iPhone user agent, it will redirect to another Duck DNS page. For an Android user agent, it will redirect to `181.html` .

This page also has an IP of 45.12.138[.]87.

Android User-Agent

Under the "Network Conditions" tab in inspect element, I set the User-Agent to,

> Mozilla/5.0 (Linux; Android 6.0; Nexus 5 Build/MRA58N) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/109.0.0.0 Mobile Safari/537.36

For an Android User-Agent, it will first lead to `/181.html`

The stream for the `181.html` GET request shows that it will redirect to another Duck DNS page.

The final Duck DNS page has an IP of 199.167.138[.]24.

The IP 199.167.138[.]24 also has many Duck DNS domains associated with it.

This final Duck DNS page shows a fake AU page with the following prompt,

> マルウェアが検出されました。「KDDIセキュリティ無料版アプリ」を必ずダウンロードしてインストールしてください。そうしないと通話サービスを停止される場合がございますのでご注意ください。

Which translates to,

> Malware was detected on your device. Please be sure to download and install the "KDDI Security Free Edition App". Please note that if you do not, the call service may be suspended.

Clicking on 次へ (next) will lead to a download page. Scrolling through the page will show the install instructions.

Clicking on "Download" will download a file called `KDDI.apk`

This `KDDI.apk` is flagged as malicious by multiple vendors on VirusTotal.

This file contacts multiple URLs, domains and IP addresses.

JoeSandbox detected `KDDI.apk` as malicious, and many suspicious behaviours can be seen.

`KDDI.apk` makes various permission requests such as `android.permission.SEND_SMS` , `android.permission.CALL_PHONE` , `android.permission.WRITE_SMS` .

The full analysis on JoeSandbox can be found here,

Automated Malware Analysis Report for KDDI.apk — Generated by Joe Sandbox

Sample Name: KDDI.apk Analysis ID: 803149 MD5: 18cf999cbb7cb9fefe8ab211c196549d SHA1…

www.joesandbox.com

iPhone User-Agent

Under the "Network Conditions" tab in inspect element, I set the User-Agent to,

> Mozilla/5.0 (iPhone; CPU iPhone OS 13_2 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) CriOS/109.0.0.0 Mobile/15E148 Safari/604.1

It leads to `index.html` , however, "404 Not Found" was displayed.

Inspecting the headers showed the following,

This page has an IP of 86.38.4[.]25, and has many other Duck DNS domains associated with it. A lot of them are flagged as malicious on VirusTotal.

Since I could not access the site's contents, I went to the `Sensors` tab and set the location to `Tokyo` , with the Locale set to `ja-JP` .

Reloading the page leads to a fake AU page that asks for the user's mail address, phone number, and name.

I entered some fake credentials and had to select a payment method. There seemed to be multiple payment options, but everything except `電子マネー` (Electronic money) was crossed out.

Submitting the credentials leads to a page that says the payment must be made using `Vプリカ` , which is a prepaid card.

It then prompts the user to enter the `Vプリカ` (prepaid card) numbers.

`Vプリカ` is a Visa prepaid card that can be used online. More details on `Vプリカ` can be found below,

Ｖプリカ | トップページ | ネット専用Visaプリペイドカード

Ｖプリカは、ネット専用Visaプリペイドカードです。インターネット上のVisa加盟店で、クレジットカードと同じように使えます。本人確認資料、審査なしですぐに発行できます。セキュリティロック、VISA認証サー ビス（3-Dセキュア）対応。

vpc.lifecard.co.jp

Duck DNS behaviour

The redirect link changes very frequently. The first link is lhuyykzzlv.duckdns[.]org in this case, but it redirects to a different Duck DNS link every few mins-hours.

The second link's redirect will also change every few mins-hours.

The first and second Duck DNS domain has an IP of 45.12.138[.]87, and has many Duck DNS domains associated with them.

As Duck DNS is a free dynamic DNS, it is often abused for malicious purposes like in this case.

Conclusion

In this investigation, it was found that the behaviour of the smishing attack differs based on the User-Agent, and abuses Duck DNS. Multiple redirects are made before it reaches the fake AU page. Accesses from certain locations will prevent the fake AU page from loading.

- Android User-Agent: Redirects the user to a fake AU page, and downloads a malicious file called `KDDI.apk`
- iPhone User-Agent: Redirects the user to a fake AU page, and asks for the user's details, and Vプリカ (prepaid card) numbers.

The behaviour of this smishing attack is similar to the one analyzed in my other blog, where it abused Duck DNS and changed behavior based on the User-Agent.

A “strange font” Smishing that changes behaviour based on User-Agent, and abuses Duck DNS

Recently in Japan, there has been an increase in Smishing attacks that uses a strange font. This got me wondering what…

medium.com

So if you receive an SMS message that uses Duck DNS, please be careful!