Grab your own copy of Phenakite iOS malware today

malware4all.blogspot.com/2021/05/grab-your-own-copy-phenakite-ios.html

Facebook has recently published a technical paper regarding a threat actor named APT-C-23.

Almost half of their report is about a new iOS malware that is in use by the threat actor.

Facebook called this malware Phenakite and provided 2 hashes of malware samples, however, those samples are not publicly available (yet).

Since I am Android type of person, naturally the Android malware interested me more than the iOS malware.

After playing a little with the Android malware, I decided to see what I can learn about the iOS malware, but how? I don't have any sample and I am quite clueless with Apple devices at every possible level. Well:

> We don’t need bombs we got fire kites

Fortunately, the distribution site of the malware was still alive:

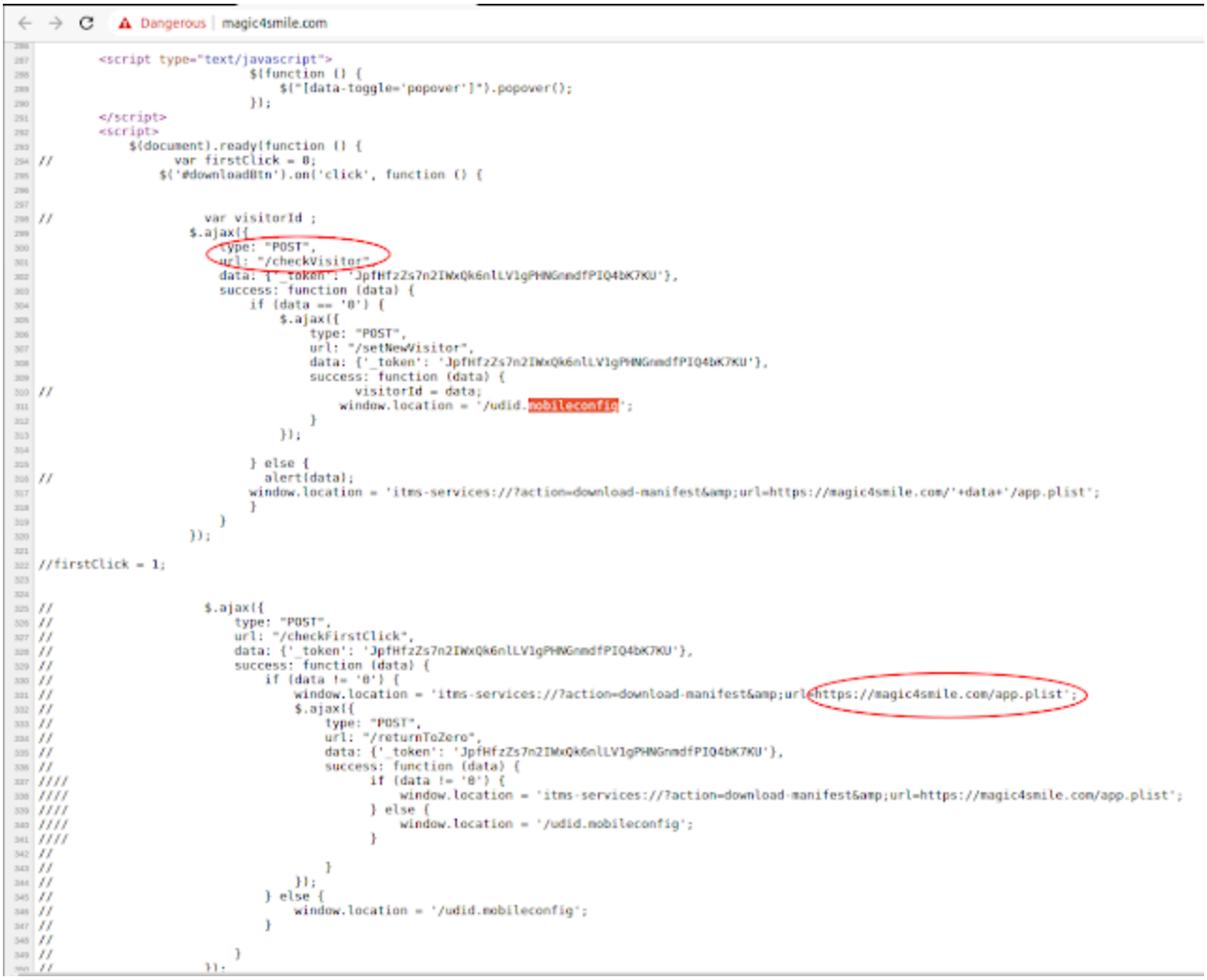
Well, not much to do other than download the app, well the link is not directly the app apparently:

```
tmf:~/Downloads$ file udid.mobileconfig
udid.mobileconfig: data
tmf:~/Downloads$ strings udid.mobileconfig | grep Dev
        <key>DeviceAttributes</key>
#Apple Worldwide Developer Relations1D0B
;Apple Worldwide Developer Relations Certification Authority0
#Apple Worldwide Developer Relations1D0B
;Apple Worldwide Developer Relations Certification Authority0
1iPhone Developer: Moustafa abughafra (AW9Z45LMLF)1
#Apple Worldwide Developer Relations1D0B
;Apple Worldwide Developer Relations Certification Authority
#Apple Worldwide Developer Relations1D0B
;Apple Worldwide Developer Relations Certification Authority
#Apple Worldwide Developer Relations1D0B
;Apple Worldwide Developer Relations Certification Authority
tmf:~/Downloads$
```

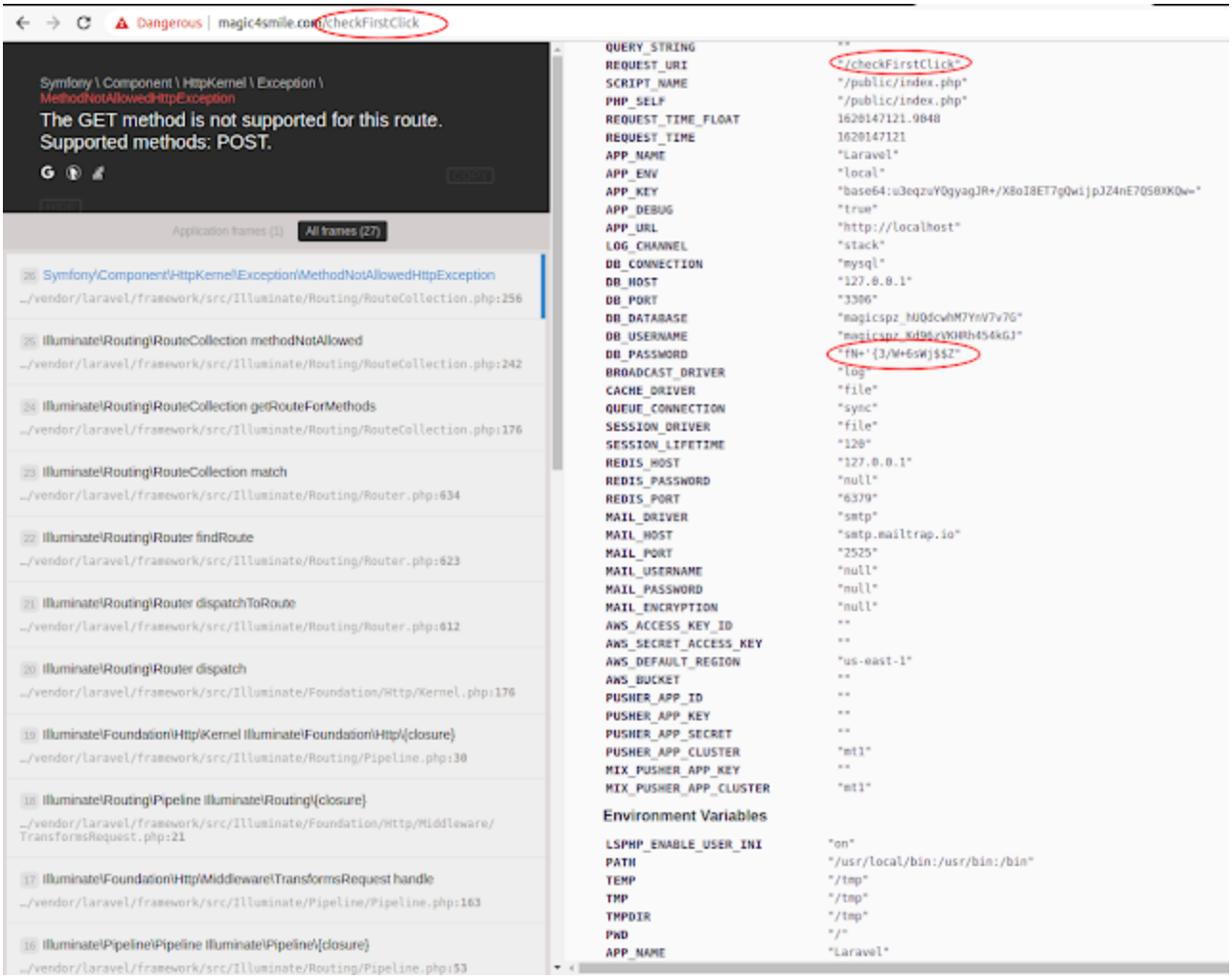
The file is binary, but also contains strings that might be interesting. There are several tools that parse mobileconfig files, a curious reader might try to parse the file for additional

information, as this probably should trigger the download of the app after the policy is accepted.
But now what?

Feeling stuck? no worries I felt the same as well. Since I don't have iOS device to try it out, I decided to inspect the code of the website:



Oh look at that, commented code, that must be good :P



WhoOpSec!

There was also a reference to a file named app.plist lets try to grab it, shall we?

```
tmf:~/Downloads$ file app.plist
app.plist: XML 1.0 document, ASCII text
tmf:~/Downloads$ cat app.plist
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
        <key>items</key>
        <array>
                <dict>
                        <key>assets</key>
                        <array>
                                <dict>
                                        <key>kind</key>
                                        <string>software-package</string>
                                        <key>url</key>
                                        <string>https://magic4smile.com//app.ipa</string>
                                </dict>
                        </array>
                        <key>metadata</key>
                        <dict>
                                <key>bundle-identifier</key>
                                <string>MagicChat.com.</string>
                                <key>bundle-version</key>
                                <string>4.0</string>
                                <key>kind</key>
                                <string>software</string>
                                <key>subtitle</key>
                                <string>41A472</string>
                                <key>title</key>
                                <string>MagicSmile</string>
                        </dict>
                </dict>
        </array>
</dict>
```

Ok, this is plain text and simple, the software package is app.ipa, lets grab that as well:

```
tmf:~/Downloads/app$ ls -lah
total 14M
drwxrwxr-x  2 sk sk 4.0K May  4 20:02 .
drwxr-xr-x 16 sk sk  92K May  4 20:02 ..
-rw-rw-r--  1 sk sk  13M Jan 13  2020 app.ipa
tmf:~/Downloads/app$ md5sum app.ipa
38283546b418ff3801ff8111459abd4a  app.ipa
```

Ah, close, but no cigar, this hash doesn't match the two samples in Facebook report.

Could it be a new sample? doubt it, look at the date. So what is this file? ipa obviously! Not to be confused with IPA.

Essentially it is a Zip file, so lets unzip that payload:

```
tmf:~/Downloads/app/Payload/app.app$ ls -lah
total 13M
drwxr-xr-x 65       20K May  4 20:12 .
drwxr-xr-x  3      4.0K Jan  4  2020 ..
drwxr-xr-x  2      4.0K Jan  4  2020 AddAccountView.nib
drwxr-xr-x  2      4.0K Jan  4  2020 AddFriendsCell.nib
drwxr-xr-x  2      4.0K Jan  4  2020 AddFriendsView.nib
drwxr-xr-x  2      4.0K Jan  4  2020 AdvertCustomView.nib
drwxr-xr-x  2      4.0K Jan  4  2020 AdvertPremiumView.nib
drwxr-xr-x  2      4.0K Jan  4  2020 AllMediaCell.nib
drwxr-xr-x  2      4.0K Jan  4  2020 AllMediaHeader.nib
drwxr-xr-x  2      4.0K Jan  4  2020 AllMediaView.nib
-rwxr-xr-x  1       12M Jan 13  2020 app
drwxr-xr-x  2      4.0K Jan  4  2020 ArchiveCell.nib
-rw-r--r--  1       523 Jan 13  2020 archived-expanded-entitlements.xcent
drwxr-xr-x  2      4.0K Jan  4  2020 ArchiveView.nib
-rw-r--r--  1      306K Jan  4  2020 Assets.car
drwxr-xr-x  2      4.0K Jan  4  2020 AudioView.nib
drwxr-xr-x  3      4.0K Jan  4  2020 Base.lproj
drwxr-xr-x  2      4.0K Jan  4  2020 BlockedCell.nib
drwxr-xr-x  2      4.0K Jan  4  2020 BlockedView.nib
drwxr-xr-x  2      4.0K Jan  4  2020 CacheView.nib
drwxr-xr-x  2      4.0K Jan  4  2020 CallAudioView.nib
drwxr-xr-x  2      4.0K Jan  4  2020 CallsView.nib
drwxr-xr-x  2      4.0K Jan  4  2020 CallVideoView.nib
drwxr-xr-x  2      4.0K Jan  4  2020 ChatsCell.nib
drwxr-xr-x  2      4.0K Jan  4  2020 ChatsView.nib
drwxr-xr-x  2      4.0K Jan  4  2020 _CodeSignature
-rw-r--r--  1       11K Jan  4  2020 countries.plist
drwxr-xr-x  2      4.0K Jan  4  2020 CountriesView.nib
drwxr-xr-x  2      4.0K Jan  4  2020 CreateGroupView.nib
drwxr-xr-x  2      4.0K Jan  4  2020 CustomStatusView.nib
drwxr-xr-x  2      4.0K Jan  4  2020 EditProfileView.nib
-rw-r--r--  1      7.4K Jan 13  2020 embedded.mobileprovision
drwxr-xr-x 25      4.0K Jan  4  2020 Frameworks
-rw-r--r--  1       719 Jan  4  2020 GoogleService-Info2.plist
-rw-r--r--  1       876 Jan  4  2020 GoogleService-Info.plist
drwxr-xr-x 40      4.0K Jan  4  2020 GoogleSignIn.bundle
drwxr-xr-x  2      4.0K Jan  4  2020 GroupsCell.nib
drwxr-xr-x  2      4.0K Jan  4  2020 GroupsView.nib
drwxr-xr-x  2      4.0K Jan  4  2020 GroupView.nib
drwxrwxr-x  2       12K May  4 20:12 img_trash
-rw-r--r--  1      4.1K Jan 13  2020 Info.plist
drwxr-xr-x  2      4.0K Jan  4  2020 KeepMediaView.nib
drwxr-xr-x  2      4.0K Jan  4  2020 LoginEmailView.nib
drwxr-xr-x  2      4.0K Jan  4  2020 LoginFaceBookViewController.nib
drwxr-xr-x  2      4.0K Jan  4  2020 LoginGoogleView.nib
drwxr-xr-x  2      4.0K Jan  4  2020 loginIcloudViewController.nib
drwxr-xr-x  2      4.0K Jan  4  2020 LoginPhoneView.nib
drwxr-xr-x  2      4.0K Jan  4  2020 MapView.nib
drwxr-xr-x  2      4.0K Jan  4  2020 MediaView.nib
drwxr-xr-x  2      4.0K Jan  4  2020 NetworkView.nib
drwxr-xr-x  2      4.0K Jan  4  2020 PasswordView.nib
drwxr-xr-x  2      4.0K Jan  4  2020 PeopleCell.nib
drwxr-xr-x  2      4.0K Jan  4  2020 PeopleView.nib
-rw-r--r--  1         8 Jan  4  2020 PkgInfo
```

I moved all the images to a folder to keep only the potentially interesting files from the archive, namely "app" stands out, what is it?

```
tmf:~/Downloads/app/Payload/app.app$ file app
app: Mach-O 64-bit arm64 executable, flags:<NOUNDEFS|DYLDLINK|TWOLEVEL|WEAK_DEFINES|BINDS_TO_WEAK|PIE>
tmf:~/Downloads/app/Payload/app.app$ md5sum app
e567efd5c800c5b0c6eb5aa0bccc10e9  app
```

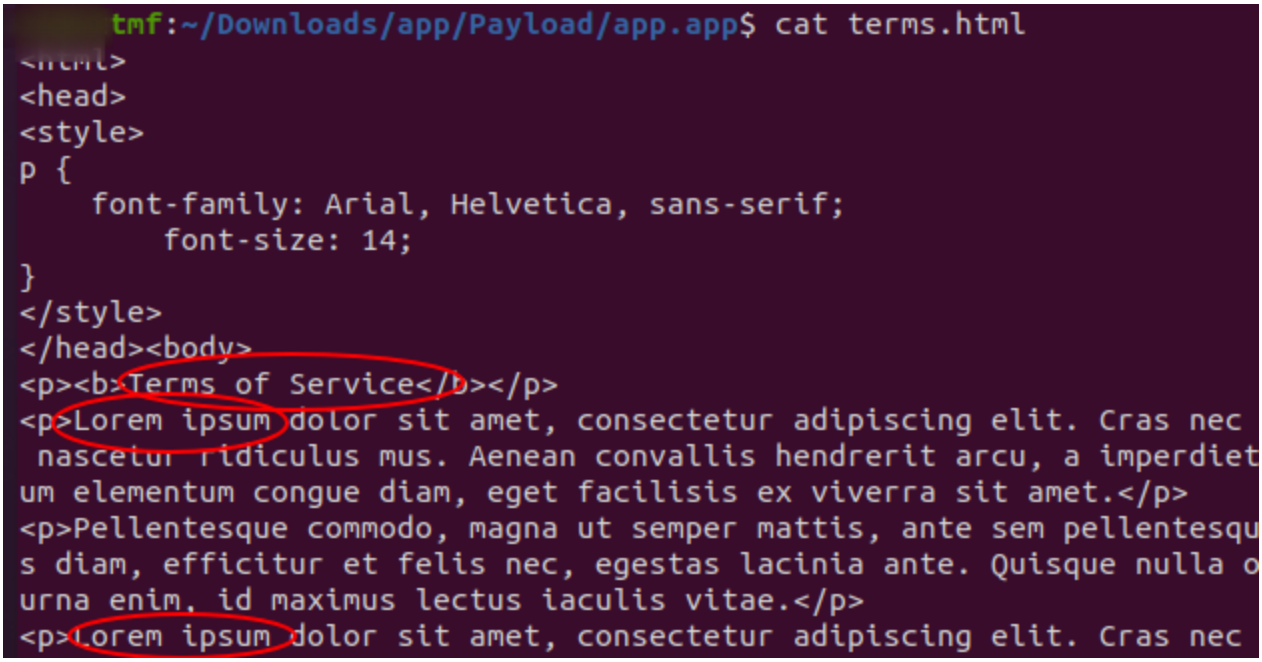
And that, kids, how I met your malware, **e567efd5c800c5b0c6eb5aa0bccc10e9** , I met her on Facebook, report.
Congratulations, this is the first time the blog actually does what it stands for, sharing malware for everyone with a hint of analysis. (if you are reading this too late and the distribution site of the malware is down, no worries, it is also available at VirusTotal as a

standalone and as an archive)

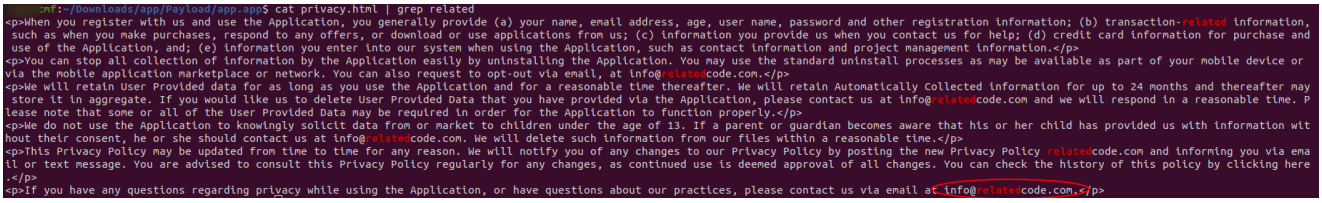
Now you can enjoy your own copy of Phenakite and start reversing the Mach-O if you know how to :)

Bonus lol's:

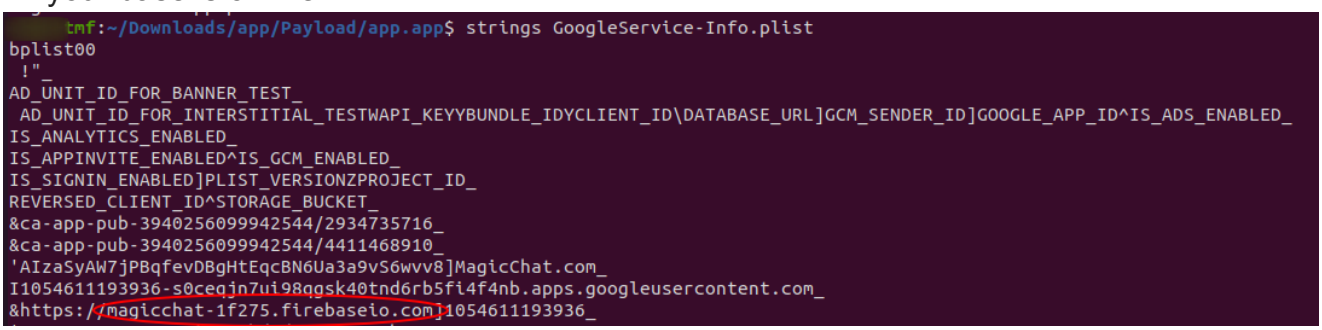
The terms of service of the malware is.... Lorem Ipsum :



The privacy is seem to be borrowed from "relatedcode.com" which has an open source chat for iOS repository, this is most likely the chat app that Facebook was referring to:



All your base is on fire:



More interesting strings:

```
tmf:~/Downloads/app/Payload/app.app$ strings embedded.mobileprovision | grep string
    <string>XC MagicChat com</string>
    <string>NA2YTWG8U2</string>
            <string>iOS</string>
            <string>NA2YTWG8U2.MagicChat.com</string>
                        <string>NA2YTWG8U2.*</string>
            <string>NA2YTWG8U2</string>
            <string>production</string>
    <string>magicChat</string>
            <string>51ff4f3a9c792240c2e203e8c168f0341ff1060e</string>
            <string>7adc7f8491635772154b25858e2536fd4304b47f</string>
            <string>e602c2d296515663adeb691ba106e5baa3a5a9d0</string>
            <string>e7274d7e737beaec58891351e7b6f6a411243f57</string>
            <string>NA2YTWG8U2</string>
    <string>roy been</string>
    <string>24761a57-9c52-4761-9a7c-ddcf92ddbd9b</string>
```

phenakite.zip
MD5: 54e5e93c00c963cb66fd2d248c4c6ce7
SHA-1: 05527dddb79329d844f1954e3d36601926410bca
SHA-256: c2d66369c974558adbcd801b409492b73ad1cb5f9f412ef3a8820f1cae526903

app

MD5: e567efd5c800c5b0c6eb5aa0bccc10e9
SHA-1: da99195ff43093fb8237201e2ce412a925580a53
SHA-256: e1494164865acb719c1e32c86adf810ce52fcc48c46e777b9f98a99648de62c2