スミッシング確認してみた

2023/10/06 勉強会@salty_byte

※スライド自体は2019/09/06に書いたもので、少しだけ手直ししています。

Q. スミッシングって？

A. こんなのです。

画像参照元:
https://piyolog.hatenadiary.jp/entry/2019/08/11/060157
https://twitter.com/tomoe1160/status/1057214125695062017
https://twitter.com/Lotus_Beijing/status/918658337532649473

正確には・・・

1. どこからか偽のSMSが届く。

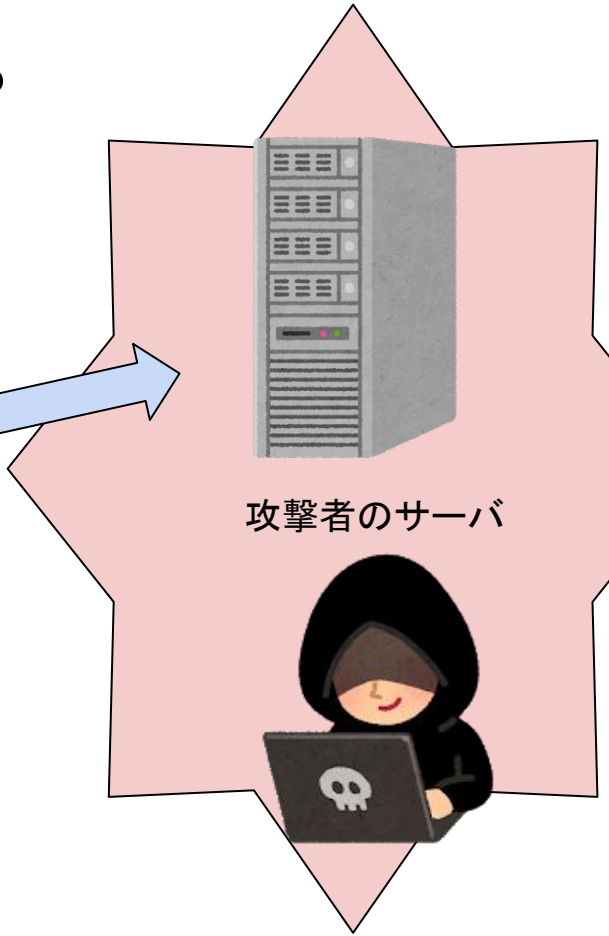
2. クリックしてしまう。


1/23/17 15:19
GoogleよりGoogleplayアカウントのお支払方法登録のお願いです。詳細はURLをクリック
http://
ぽちっ

3. それっぽい画面が表示される。

4. 本物と思って情報を入力してしまう。

5. 入力した情報がどこかに送られる。



です。

画像元：
https://blog.trendmicro.co.jp/archives/tag/%E3%82%B9%E3%83%9F%E3%83%83%E3%82%B7%E3%83%B3%E3%82%B0

スミッシング（Smishing）とは

SMSを利用したフィッシング詐欺のこと。

SMSフィッシング（SMS phishing）から来た造語である。

フィッシングサイトに誘導し、情報の窃取やマルウェア感染を狙う。

スミッシング被害

- 最近スミッシング攻撃が激化している。
  - 2018年1～3月には123件 ⇒ 2018年10～12月には4万3982件
- 金融犯罪にご注意ください /三菱UFJ銀行
- 宅配便業者をかたる偽ショートメッセージに関する相談が急増中、誘導されるまま Android端末にアプリをインストールしないように！ /IPA
- 偽SMSで個人情報狙う「スミッシング」が激化 携帯事業者装い新手口も /産経ニュース
- グーグル装い「スミッシング」で詐欺 PCからカード情報200件 警視庁 /産経ニュース
- ドコモを装うスミッシング -「高額料金発生」と不安煽る
- auアカウントを狙うスミッシングについてまとめてみた

参考:
https://www.itmedia.co.jp/news/articles/1904/16/news055.html
https://cybersecurity-jp.com/cyber-terrorism/31203
http://www.security-next.com/106850
https://piyolog.hatenadiary.jp/entry/2019/08/11/060157

ところで・・・

実際のところ攻撃は難しいのでは？

- SMSって送るのに電話番号必要では？
- 送信者を偽装できないのでは？
- ガラケー利用者で、スマホは使ってないから安心？

実際のところ攻撃は難しいのでは？

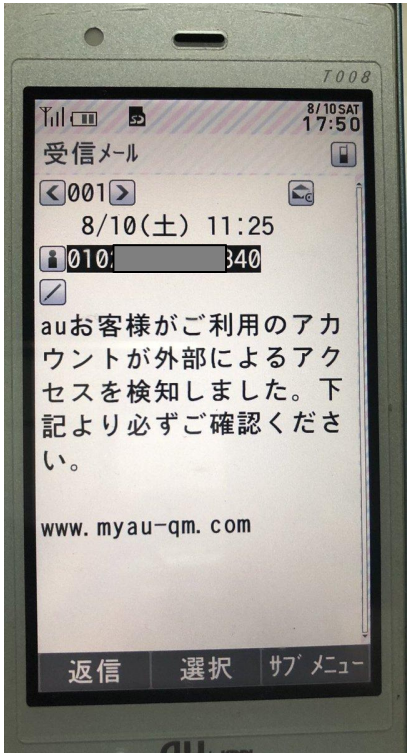
- SMSって送るのに電話番号必要では？
  - SMS対応SIM買えばいい。
  - クラウド電話サービスなるものがある。(Twilio等)
  - SMS送信サービスなるものがある。(メディア SMS等)
  - マルウェアに感染させて、他人のスマホを使う。
- 送信者を偽装できないのでは？
- ガラケー利用者で、スマホは使ってないから安心？

実際のところ攻撃は難しいのでは？

- SMSって送るのに電話番号必要では？
- 送信者を偽装できないのでは？
  - キャリアやサービスにもよるが、SMS受信時に表示される送信者 ID（Sender ID）は任意に指定することが可能な場合がある。
  - 詳しくは：https://akaki.io/2019/sms_spoofing.html
- ガラケー利用者で、スマホは使ってないから安心？

実際のところ攻撃は難しいのでは？

- SMSって送るのに電話番号必要では？
- 送信者を偽装できないのでは？
- ガラケー利用者で、スマホは使ってないから安心？
  - ガラケーでもSMS対応している場合、狙われる。
  - 逆に言うと、SMS対応していない場合は問題ないと思われる。
    - 当然通常のフィッシングには注意する必要はある。



デモ

まとめ

- スミッシングは**SMS**を利用したフィッシング詐欺のこと。
- （キャリアにもよるが）正規の会社を装うことは難しくない。
- SMSなので、ガラケー利用者でも注意が必要。

まとめ

- 内容にURLが入っていたら、不用意にクリックしない。
- 気になる内容だったら、Google検索やX等で同じことが発生していないか検索する。
- どうしてもアクセスしたい場合は、「https://securl.nu/」のようなサービスで確認してみると面白いかも。
    - idとか重要情報が含まれていないことを確認してからにすること

X

安全なSMS生活を！

参考

https://piyolog.hatenadiary.jp/entry/2019/08/11/060157

https://akaki.io/2019/sms_spoofing.html