Why your Cellphone is not as secure as you think

Name: Brandon Harris

Class: Public Speaking

Teacher: Professor Watts

Disclaimer!

Any thing learned or seen in this presentation is public information and if the information learned here is used in any illegal way, I assume no responsibility or liability for the actions that you may commit.

Introduction

Have you ever wondered if someone could see all the activity that you do on your phone everyday from:

- Online Banking
- Social Media
- The photos you take
- The text you send

Well In this Presentation I will show you someone can and how you can protect your self from people who may have malicious intent towards.

Objectives

- The audience will be will learn about:

- Different attack methods to take information from there phones

•Real life use cases of how hackers or intelligence agencies such as the NSA, CIA, or FBI can gain access phones or take information off them

•How to keep the information that they keep on their phone safe

A Few Definitions Before we Begin

- Phishing – Crafting a legitimate looking email with a malicious link in order to collect user information such as passwords, email address, phone number, social security number

- Smishing – phishing through text messages so instead of an email it would be a text with a malicious link

- Lockheed Martian Cyber Kill Chain – Developed by the Defense contractor Lockheed Martian and is a model for the identification and prevention of cyber attacks involves Reconnaissance, weaponization, Delivery, Exploitation, Installation, command and control, and Action on Objectives.

- Vulnerability – weakness of hole in security

- Malware – Malicious software

- Spyware – Malware that can collect what you type of your keyboard, emails or text that you send, and can access your camera without permission

Let The Games Begin

- Ever good Cyber Attack starts of with some form of Reconnaissance whether that:

- social engineering such as going up to with a simile and asking for your first and last name or phone number outright

- Looking a name tag you may have on or Asking a friend of yours for you full name

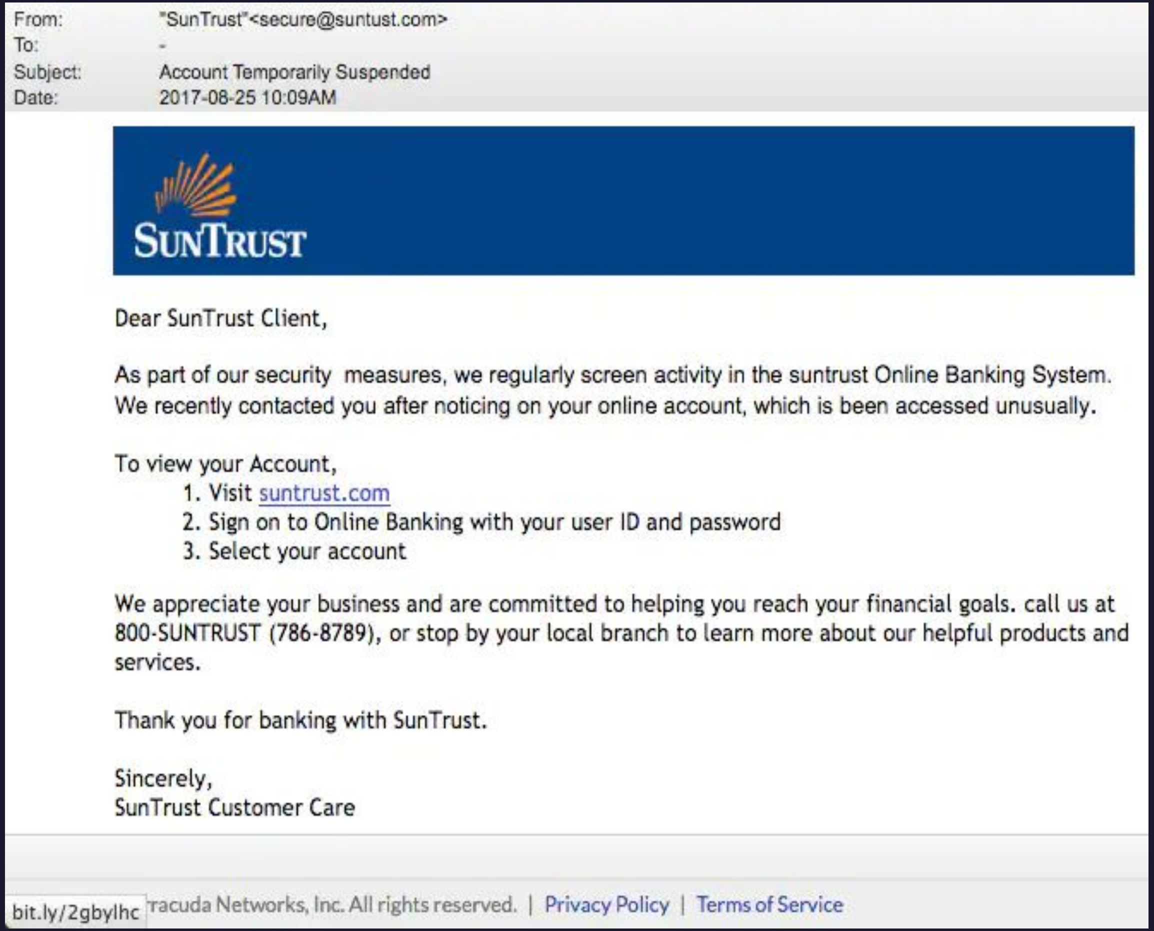
Once an attackers has basic collected information, they need from you in this stage they can enter your name into google or in "certain websites" to see your phone number, what social media profiles you have to see your interest are, where you live, who you are related to, or what job you have.

Let's Get One thing straight

People like me don’t need to get Close to your phone to get information off it or from you

Examples

PHISHING EMAIL



From: "SunTrust"<secure@suntust.com>
To: -
Subject: Account Temporarily Suspended
Date: 2017-08-25 10:09AM

Dear SunTrust Client,

As part of our security measures, we regularly screen activity in the suntrust Online Banking System. We recently contacted you after noticing on your online account, which is been accessed unusually.

To view your Account,

1. Visit suntrust.com
2. Sign on to Online Banking with your user ID and password
3. Select your account

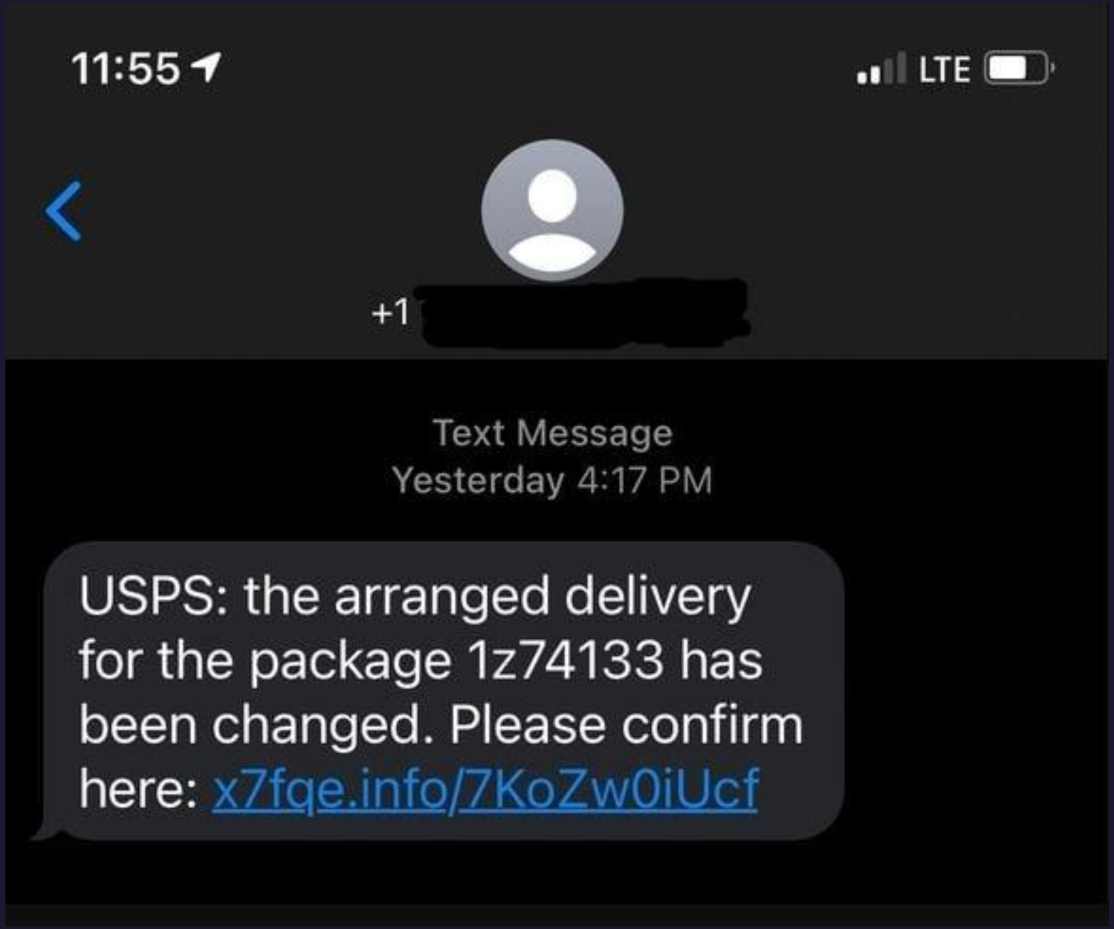
We appreciate your business and are committed to helping you reach your financial goals. call us at 800-SUNTRUST (786-8789), or stop by your local branch to learn more about our helpful products and services.

Thank you for banking with SunTrust.

Sincerely,
SunTrust Customer Care

bit.ly/2gbylhc racuda Networks, Inc. All rights reserved. | Privacy Policy | Terms of Service

SMISHING TEXT MESSAGE



+1 [redacted]

Text Message
Yesterday 4:17 PM

USPS: the arranged delivery for the package 1z74133 has been changed. Please confirm here: x7fqe.info/7KoZw0iUcf

How To can Gain Access to your Phone directly

- Spyware is legal(kid tracking app) and illegal mainly used by stalkers or intelligence agencies for example Pegasus spyware which was created by the NSO an Israeli cyber arms firm with close ties to Israels unit 8200 government hacking group(equivalent to NSA TAO or Equation group) can be installed on your phone through a meme that you click on and can

- Listen through your microphone, look at and take photos of you, can collect basically all the information on your phone

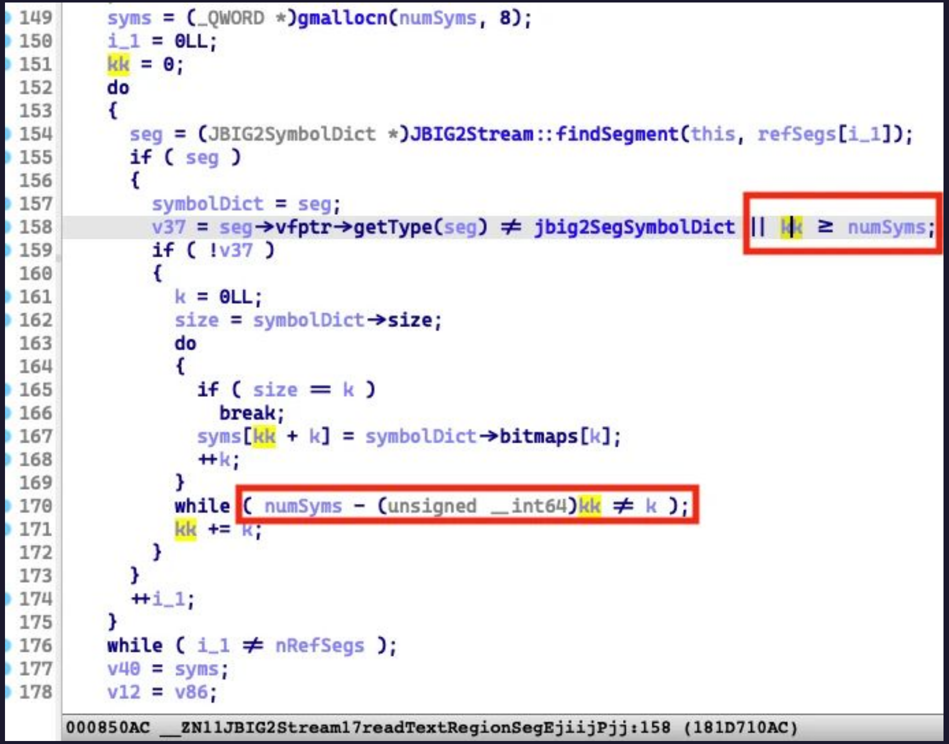
- Fake charging Cables, you plug up phone up with a fake charger I give you it can install spyware on your phone where I will be able to collect its password and all saved information on it like your photos and your credit information

- Software Flaw – If you have a venerable version of an iPhone, I can send you a text message with an exploit in it which will give me full access to your phone

- Brute Forcing – this involves me taking your phone away from you and trying to crack its password by guessing one digit at a time

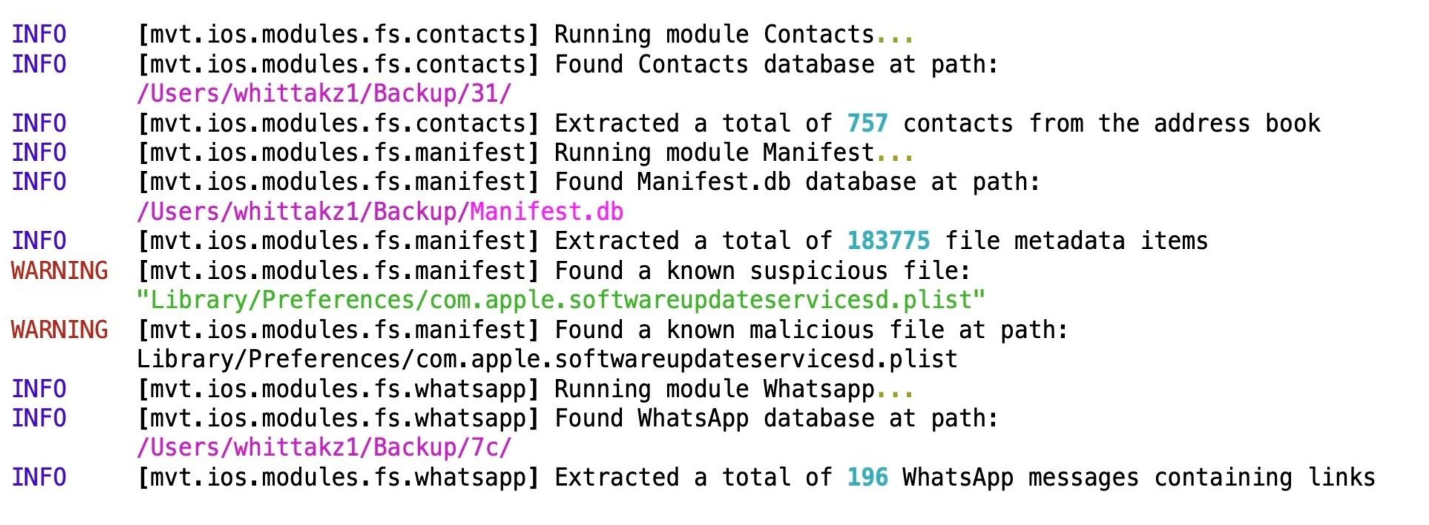
Examples

ZERO CLICK EXPLOIT – VULNERABILITY THAT WAS IN IPHONES THAT ALLOWED FOR READING USERS TEXT MESSAGES(PART OF PEGASUS SPYWARE) CODE BRUTE FORCED IT WAY PASS THE SECURITY OF IMESSAGE



```
    syms = (_QWORD *)gmallocn(numSyms, 8);
    i_1 = 0LL;
    kk = 0;
    do
    {
      seg = (JBIG2SymbolDict *)JBIG2Stream::findSegment(this, refSegs[i_1]);
      if ( seg )
      {
        symbolDict = seg;
        v37 = seg→vfptr→getType(seg) ≠ jbig2SegSymbolDict || kk ≥ numSyms;
        if ( !v37 )
        {
          k = 0LL;
          size = symbolDict→size;
          do
          {
            if ( size == k )
              break;
            syms[kk + k] = symbolDict→bitmaps[k];
            ++k;
          }
          while ( numSyms - (unsigned __int64)kk ≠ k );
          kk += k;
        }
      }
      ++i_1;
    }
    while ( i_1 ≠ nRefSegs );
    v40 = syms;
    v12 = v86;
000850AC __ZN11JBIG2Stream17readTextRegionSegEjiijPjj:158 (181D710AC)
```

PEGASUS SPYWARE



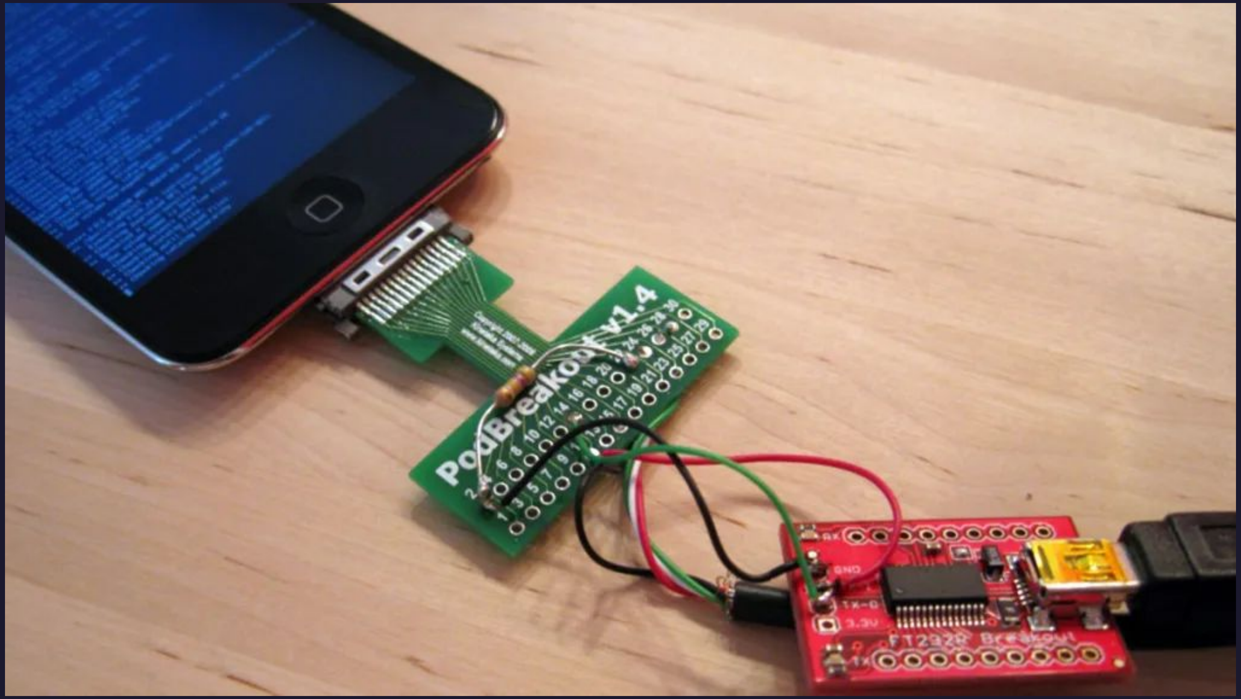
```
INFO      [mvt.ios.modules.fs.contacts] Running module Contacts...
INFO      [mvt.ios.modules.fs.contacts] Found Contacts database at path:
          /Users/whittakz1/Backup/31/
INFO      [mvt.ios.modules.fs.contacts] Extracted a total of 757 contacts from the address book
INFO      [mvt.ios.modules.fs.manifest] Running module Manifest...
INFO      [mvt.ios.modules.fs.manifest] Found Manifest.db database at path:
          /Users/whittakz1/Backup/Manifest.db
INFO      [mvt.ios.modules.fs.manifest] Extracted a total of 183775 file metadata items
WARNING   [mvt.ios.modules.fs.manifest] Found a known suspicious file:
          "Library/Preferences/com.apple.softwareupdateservicesd.plist"
WARNING   [mvt.ios.modules.fs.manifest] Found a known malicious file at path:
          Library/Preferences/com.apple.softwareupdateservicesd.plist
INFO      [mvt.ios.modules.fs.whatsapp] Running module Whatsapp...
INFO      [mvt.ios.modules.fs.whatsapp] Found WhatsApp database at path:
          /Users/whittakz1/Backup/7c/
INFO      [mvt.ios.modules.fs.whatsapp] Extracted a total of 196 WhatsApp messages containing links
```

Exacting Information from WhatsApp a instant messaging application

More Examples

FAKE CHANGING CABLE – ONLY COST $99 DOLLARS

SAN BERNADINO IPHONE – THE SAN BERNADINO MILITARY BASE SHOOTER IPHONE PASSWORD WAS CRACKED BY THE FBI HACKING TEAM (ROU OR RAT) AFTER APPLE REFUSED TO UNLOCK THE PHONE AND NSA REFUSED TO HELP



Wrote code that got rid of the data erase feature or password time out feature when a password is entered to many times

How to keep yourself Safe

- Make Sure that your phone is updated and install updates immediately don't wait.
- If you get an email or text message asking for your information, offering some type of discount or reward verify it by calling your bank, family member, work, and logging into your amazon, social media or brand apps.
- Beware of what information that you are giving out to people of giving to websites online
- Don’t post to much personal information on your social media
- Have strong passwords or change your passwords ever so often(not really stopping a dedicated attacker tho) but it’s important

Summary

Your phone is access into your personal secrets, and life in general don't trust everyone with it or your information just because you don’t think this stuff happens only in movies and I haven’t touched how I can used Bluetooth against you so protect your information.

Any Questions?

References

- Tarrad, K. M., Al-Hareeri, H., Alghazali, T., Ahmed, M., Al-Maeeni, M. K. A., Kalaf, G. A., Alsaddon, R. E., & Mezaal, Y. S. (2022, July 2). *CyberCrime Challenges in Iraqi Academia: Creating Digital Awareness For Preventing Cyber Crime.* View of cybercrime challenges in Iraqi academia: Creating Digital Awareness for Preventing Cybercrimes. Retrieved March 19, 2023, from https://cybercrimejournal.com/menuscript/index.php/cybercrimejournal/article/view/87/24

- 15, B. M. J. S., Authors, Analyst, M. J. T., Jin, M., Analyst, T., & Us, C. (2021, September 15). *Analyzing pegasus spyware's zero-click iPhone Exploit Forcedentry.* Trend Micro. Retrieved March 22, 2023, from https://www.trendmicro.com/tr_tr/research/21/i/analyzing-pegasus-spywares-zero-click-iphone-exploit-forcedentry.html

- Lutkevich, B. (2022, October 14). *What is a Wi-Fi Pineapple?* Security. Retrieved March 22, 2023, from https://www.techtarget.com/searchsecurity/definition/Wi-Fi-Pineapple

- *How to prevent phone hacking and protect.* Webroot. (n.d.). Retrieved March 22, 2023, from https://www.webroot.com/us/en/resources/tips-articles/how-to-prevent-phone-hacking-and-sleep-like-a-baby-again