“A day in the life of a script kiddie – pwning Android for the lulz”
Stuff we’ll be looking at today

- Introduction
- A short game!
- Beginning – the current state of things
- Middle – what why and how?
- End – what we learnt?
Introduction

• My name is Leum*
• I’m an IT Security Analyst**
• I work for [REDACTED]
• I look nothing like this;

*yes, it really is spelt like that, my dad was a mechanic, it’s got something to do with Petroleum!

**I break [computer] stuff for a living
Game Time!

*have you noticed how awesome my wizzy slides are yet?

**turns out I’m rubbish at Powerpoint!
The beginning bit!

- Android is ‘secure enough’
- Permissions must be granted to apps
- Google’s Play store keeps you safe
- Users can (in the main) be trusted
A couple of cool graphics I pinched from lifehacker.com
And here’s the other one*

*both are a bit out of date, but I think they illustrate the point, even if the numbers aren’t current
The End of the Beginning!

• That stuff from above just doesn’t sit well with me!
• Who actually questions the permissions?*
• Google’s Play store doesn’t keep you safe**
• Users can’t be trusted *(but to be fair, most users simply don’t have the technical understanding necessary to fairly evaluate device security)*

*I believe Android permissions are just the EULA of the mobile world

**See next slide
Google’s Play Store, not so safe!

87 fake Minecraft mods exposed Android users to scammy websites, aggressive ads

So about those permissions...

David Bisson | March 27, 2017 10:26 am | Filed under: Android, Google, Malware

134 SHARES

Google has removed 87 fake Minecraft mods from its Play Store that exposed Android users to scammy websites and aggressive ads.

The fake applications, which were reported to Google between 16 March and 21 March, fall into two categories. First, 14 of them display out-of-app advertisements to users. They do so via the same ad-displaying downloader known as "Android/TrojanDownloader.Agent_JL."
The Short Version: Android Is Secure...Users Aren't

• So given that we have a weak link, just how hard is it to ‘pwn’ an Android device?
The middle bit

Tonight Matthew, I’m going to be…

...a script kiddie!
Building the test environment*

- Find some spare mobile phones
- Patch them up to date
- Install Windows**
- Find a cool desktop wallpaper!
- Install a bunch of H@x0R sounding apps that I’ll never use but look cool!

*In a VM of course, let's not trust Malware!

**eugh!
Windows virtual machine
Researching Android RATs

• RAT = ‘Remote Access Trojan’ or ‘Remote Administration Tool’
• Where do you find such things?
• How much do they cost?
• Where to start?
• ...to the Dark Web!*

*because that’s where all the cool stuff is!
Welcome to Tor Browser
You are now free to browse the internet anonymously.

Test Tor Network Settings

Search securely with DuckDuckGo.

What Next?
Tor is NOT all you need to browse anonymously! You may need to change some of your browsing habits to ensure your identity stays safe.
- Tips On Staying Anonymous
- Tor Browser User Manual

You Can Help!
There are many ways you can help make the Tor Network faster and stronger:
- Run a Tor Relay Node
- Volunteer Your Services
- Make a Donation

The Tor Project is a US 501(c)(3) non-profit dedicated to the research, development, and education of online anonymity and privacy. Learn more about the Tor Project.
Built in search (DuckDuckGo)
Surely it can’t be that easy?
No way!?
It really can be that easy!
Imaginary Training Montage!

- Push-ups*
- Running**
- Karate***
- To the tune of Eye of the Tiger****

*lots of
**some
***seriously Leum? Who do you think you’re kidding?
****I couldn’t afford the royalty payment so you’ll have to use your imagination!
Demo time!

- This will probably go horribly wrong!
- If I found time then there will be a video*

  *I almost certainly didn’t get time to do this!
The end bit

- Caveats;
  - This demo was slightly simplified to make it work in this environment. Port forwarding and Dynamic DNS configuration is required to make it work in real life
  - Social Engineering is key to the success of this attack. Success rates can be improved through targeting and tailoring
What have we learnt?

- Attackers really don’t need a lot of skill, just a motive
- The attack only needs to work occasionally, and may not even be attacking your company directly (collateral damage)
- Enterprise tools may encrypt data and scan for malware, but they don’t stop calls being recorded or the phone being used as a remote mic (bug)
- If the user is trusted, then the Android security model breaks
- Defence is about educating users, not buying more ‘toys’
Additional

• The global market for Bring Your Own Device (BYOD) and enterprise mobility is expected to quadruple in size over the next four years, hitting $284 billion by 2019

• Do not blindly trust the things that vendors sell you, mobile device management, remote wipe, device encryption all mean very little if the user can’t be trusted

• BYOD or COPE without mobile device management is just plain risky!
Any questions?

- Thank you for your time! I hope you found something useful here

- I’ll be around for a little while in the networking area if you want to chat later, but I have to run for a train around 20:00, feel free to find me on LinkedIn if it’s easier*

  *it’s not hard to find me, there are only so many people called Leum in the UK :)*