

“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!

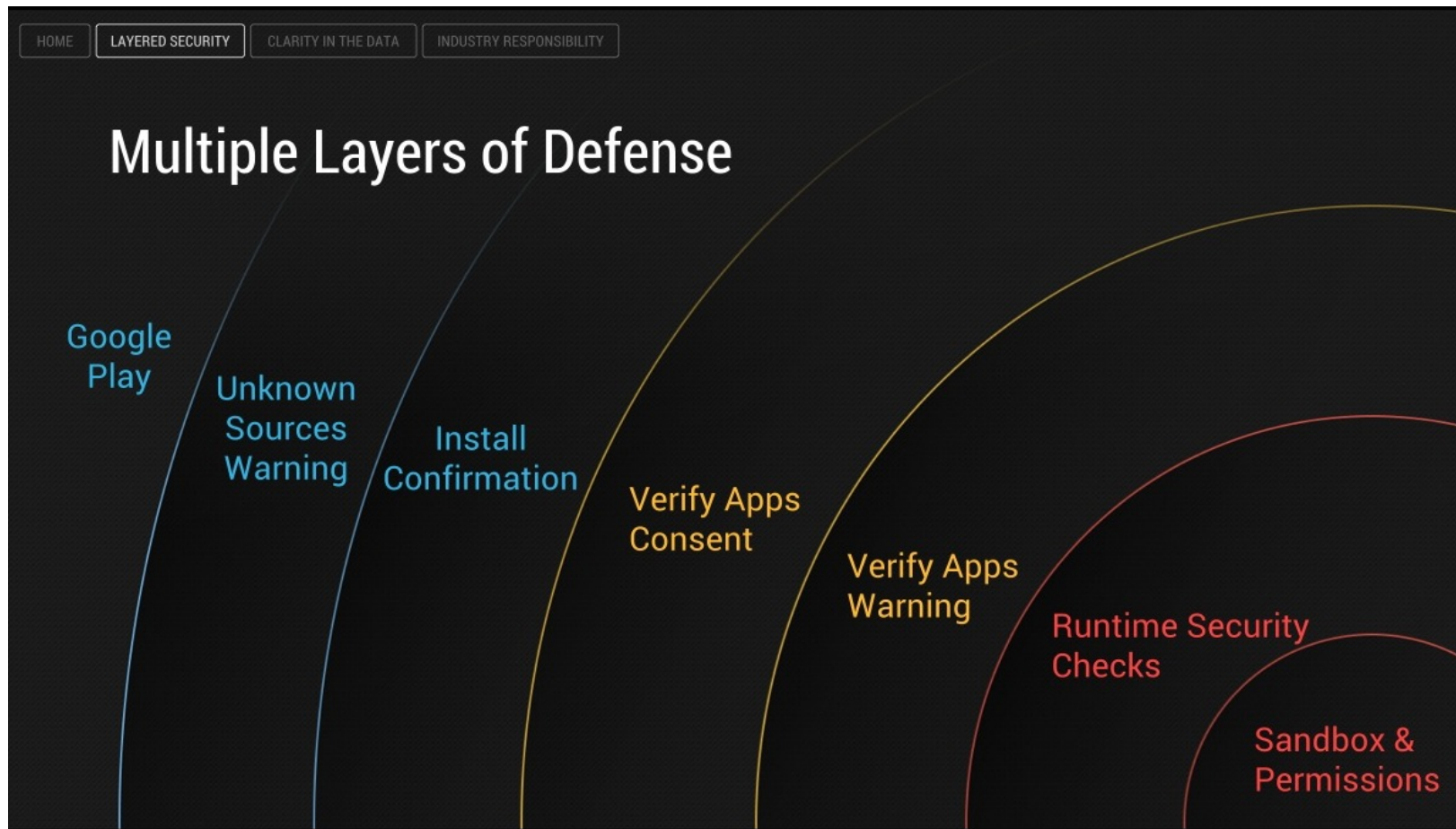
**have you noticed how awesome my wizzy slides are yet?*

***turns out I'm rubbish at Powerpoint!*

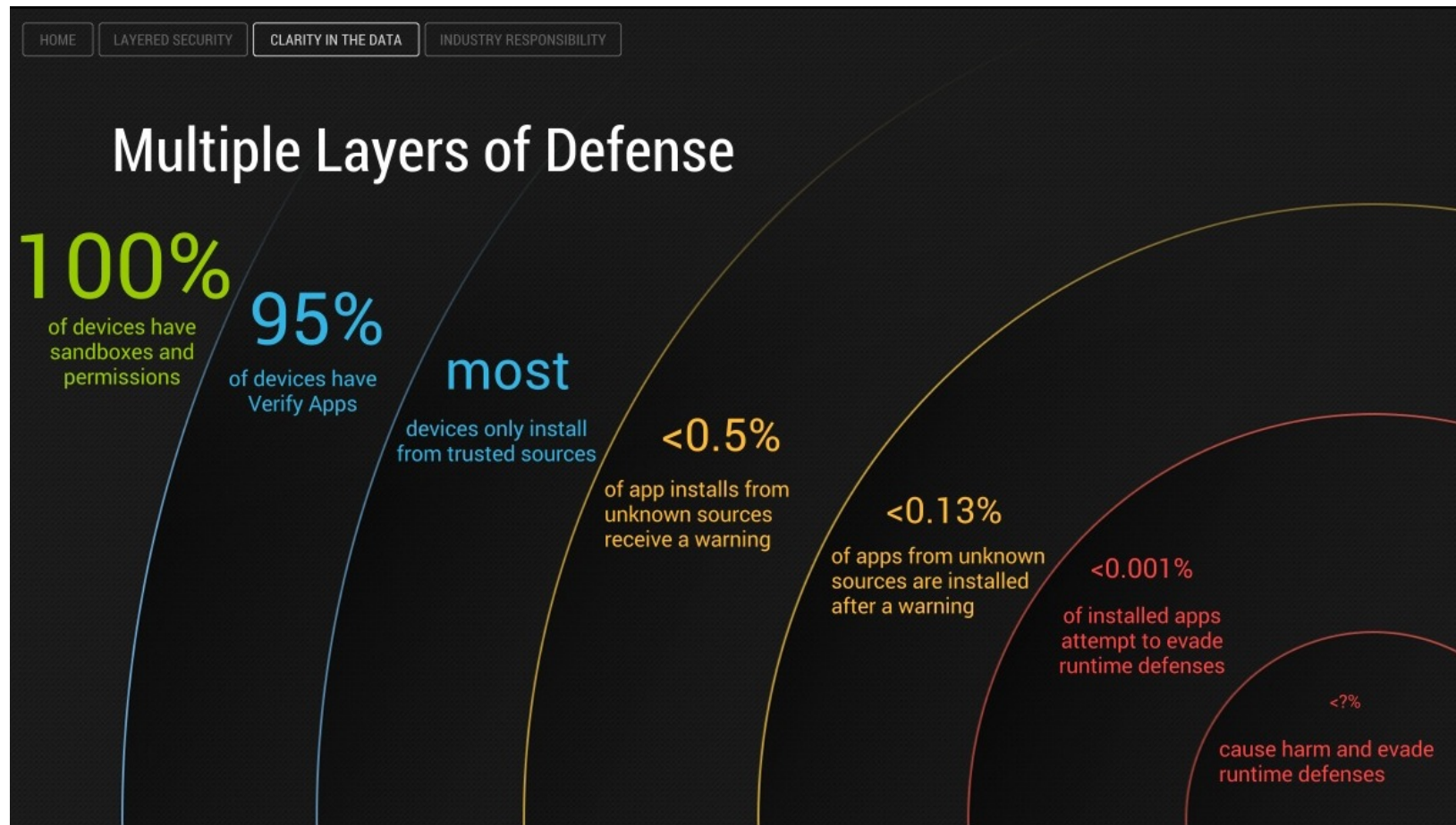
The beginning bit!

- 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**both are a bit out of date, but I think they illustrate the point, even if the numbers aren't current*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!

**GRAHAM CLULEY**
award-winning computer security news, advice and opinion


 57,929  14,336  2,626  15k 




News Newsletter Videos Podcasts Speaking Sponsor About 

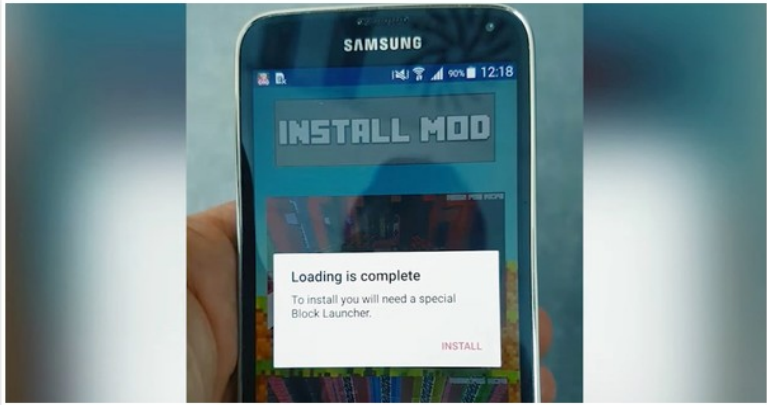
This week's sponsor: Get trending info on hackers, exploits, and vulnerabilities every day for FREE with the Recorded Future Cyber Daily.

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  0

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."

Stay informed with our free GCHQ newsletter

Over 75,000 people follow Graham Cluley for news and advice about computer security and internet privacy.

Latest videos



What happened to the Smashing Security videos?

January 25, 2017



One billion affected by Yahoo hack - LIVE STREAM

December 15, 2016



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!*

TOR

About Tor

Tor Browser | Search or enter address

Tor Browser 6.5.1



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)

The screenshot shows a web browser window with the address bar displaying "https://duckduckgo.com/?ia=videos". The search bar contains the text "android RAT". Below the search bar, there are tabs for "Web", "Images", and "Videos", with "Videos" selected. The search results are titled "Results for android RAT" and include a "More Videos" button. Four video thumbnails are displayed, each with a title, duration, and view count:

- How to setup an Android RAT (DroidJack)** - 16:36 - 172,932 views
- Setup Pupy RAT for Windows, Linux and Android - ...** - 9:40 - 16,984 views
- ANDORAT - ANDROID RAT - DEMO** - 5:37 - 29,417 views
- Взлом ОС Android - AhM Android RAT 2017** - 122,592 views

Below the video results, there are filters for "All Regions", "Any Time", and "Safe Search: Strict". A "Send feedback" button is also present. The search results list includes:

- SpyNote V3.2 - Android RAT - YouTube**
Spy Note is a free **Android RAT** with great features. Its similar to other **Android RAT**'s but it has more option and better stability. Features:
<https://youtube.com/watch?v=S1wuxIayys>
- spyNote v3.2 Stabil Android Rat THT Tested - YouTube**
SpyNote 3.2 | 2017 **Android RAT** Türkçe Anlatım Turkhackteam.org //20071999 - Duration: 17:39.
Pisikopat Bilgisayar 483 views, 17:39.
<https://youtube.com/watch?v=58KyBcgLzZc>
- The Rats Download - The Rats 3.21.2 (Android) Free Download ...**
Download The Rats 3.21.2 (Android) For Free on Mobogenie.com.*** Attention! Rat-tastic Action Game!
*** Play with 8 million players on Facebook, on your mobile or ...
mobogenie.com/download-the-rats-4929726.html
- Spaceship Rotation - Android Apps on Google Play**
Requires **Android**. 2.3 and up . Content Rating. Everyone. Learn more. Permissions. View details.
Report. Flag as inappropriate. Offered By. **RAT** Interactive ...
<https://play.google.com/store/apps/details?id=com.RATInteractive....>
- Rat On A Jet Ski | TwoAPK**
Download apk for **Android** with TwoAPK downloader. NoAds, Faster apk downloads and apk file update speed. ... **Rat On A Jet Ski**. Donut Games Install.
<https://twoapk.com/app/com.donutgames.ratonajetski/rat-on-a-...>

Surely it can't be that easy?

android RAT at DuckDuckGo

https://duckduckgo.com/?ia=videos

android RAT

Web Images Videos

Results for android RAT

More Videos

How to setup an Android RAT (DroidJack) 16:36
172,932 views

Setup Pupy RAT for Windows, Linux and Android - ... 9:40
16,984 views

ANDORAT - ANDROID RAT - DEMO 5:37
29,417 views

Взлом ОС Android - AhM Android RAT 2017 122,592 views

All Regions Any Time Safe Search: Strict Send feedback

SpyNote V3.2 - Android RAT - YouTube ←
Spy Note is a free Android RAT with great features. Its similar to other Android RAT's but it has more option and better stability. Features:
<https://youtube.com/watch?v=sSiwuxlayys>

spyNote v3.2 Stabil Android Rat THT Tested - YouTube
SpyNote 3.2 | 2017 Android RAT Türkçe Anlatım Turkhackteam.org //20071999 - Duration: 17:39.
Pisikopat Bilgisayar 483 views. 17:39.
<https://youtube.com/watch?v=58KyBcgLzZc>

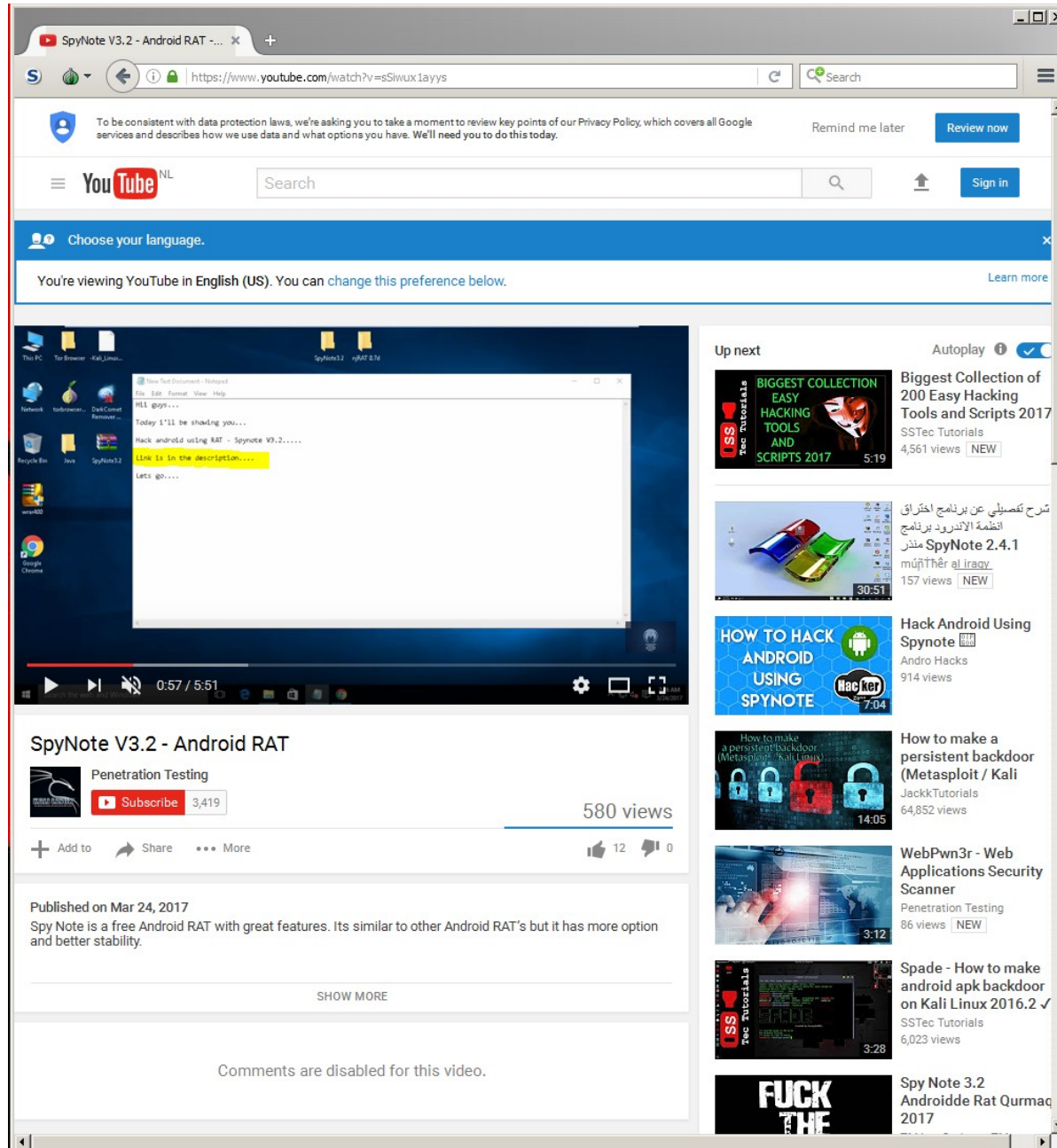
The Rats Download - The Rats 3.21.2 (Android) Free Download ...
Download The Rats 3.21.2 (Android) For Free on Mobogenie.com.*** Attention! Rat-tastic Action Game!
*** Play with 8 million players on Facebook, on your mobile or ...
mobogenie.com/download-the-rats-4929726.html

Spaceship Rotation - Android Apps on Google Play
Requires Android. 2.3 and up . Content Rating. Everyone. Learn more. Permissions. View details.
Report. Flag as Inappropriate. Offered By. RAT Interactive ...
<https://play.google.com/store/apps/details?id=com.RATInteractive....>

Rat On A Jet Ski | TwoAPK
Download apk for Android with TwoAPK downloader. NoAds, Faster apk downloads and apk file update speed. ... Rat On A Jet Ski. Donut Games Install.
<https://twoapk.com/app/com.donutgames.ratonajetski/rat-on-a-...>

Top Result!

No way!?



The screenshot shows a YouTube video player interface. The video title is "SpyNote V3.2 - Android RAT". The video content is a desktop recording of a terminal window. The terminal text includes: "Today I'll be showing you...", "Hack android using RAT - Spynote V3.2.....", "Link is in the description.....", and "Lets go....". A text document window is also open on the desktop, containing the text: "All guys...", "Today I'll be showing you...", "Hack android using RAT - Spynote V3.2.....", "Link is in the description.....", and "Lets go....". The video player shows 580 views and was published on Mar 24, 2017. The description states: "Spy Note is a free Android RAT with great features. Its similar to other Android RAT's but it has more option and better stability." The video player also shows a "Comments are disabled for this video." message.

Up next

- Biggest Collection of 200 Easy Hacking Tools and Scripts 2017
- تشرح تفصيلي عن برنامج اختراق أنظمة الأندرويد برنامج SpyNote 2.4.1 منذر
- Hack Android Using Spynote
- How to make a persistent backdoor (Metasploit / Kali)
- WebPwn3r - Web Applications Security Scanner
- Spade - How to make android apk backdoor on Kali Linux 2016.2
- Spy Note 3.2 Androidde Rat Qurmac 2017

It really can be that easy!

The screenshot shows a YouTube video player for the video "SpyNote V3.2 - Android RAT". The video player is currently at 0:57 / 5:51. Below the video player, the video title "SpyNote V3.2 - Android RAT" is displayed, along with a "Penetration Testing" category, a "Subscribe" button with 3,419 subscribers, and 580 views. The video description includes the following text:

Published on Mar 24, 2017
Spy Note is a free Android RAT with great features. Its similar to other Android RAT's but it has more option and better stability.

Features:
-No root access required
-Bind SpyNote APK server with any other APP
-Install any APK and update server
-Copy files from device to computer
-View all message on the device
-Listen to call conversations made on the device
-View contacts
-Listen live or record audio from the device microphone
-View device location
-Builder

Download: <https://drive.google.com/file/d/0B00S...>

It is for educational purpose only...

Thanks for watching...

Like share & subscribe...

Category: Education
License: Standard YouTube License

A red handwritten note "Tea Hee!" with an arrow points to the download link. The video player interface includes a search bar, a "Sign in" button, and a "Review now" button. The video player is embedded in a browser window with the address bar showing "https://www.youtube.com/watch?v=sSiwux1ayys".

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!*

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 :)*