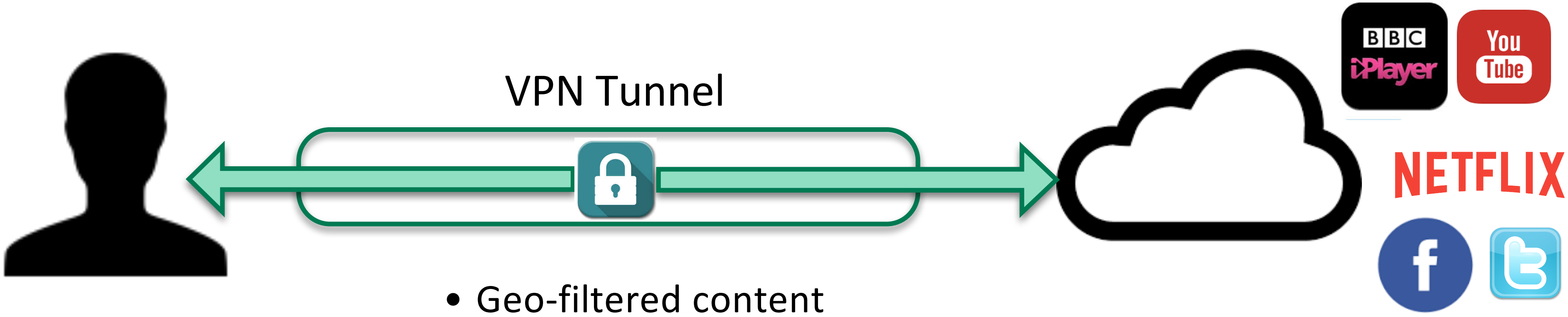
An Analysis of the Privacy and Security Risks of Android VPN Permission-enabled Apps

Muhammad Ikram (UNSW, Data61, CSIRO)
Narseo Vallina-Rodriguez (ICSI, IMDEA Networks)
Suranga Seneviratne (Data61, CSIRO)
Mohamed Ali Kaafar (Data61, CSIRO)
Vern Paxson(UC Berkeley, ICSI)

Typical VPN Use Cases



- Geo-filtered content
- Anti-surveillance
- Censorship
- Untrusted networks

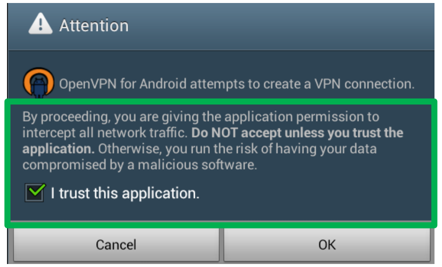
Android VPN API

- Available since Android ≧ 4.0 (Ice Cream Sandwich)
- Highly sensitive API

+ Protected by BIND_VPN_SERVICE

+ Requires user’s direct action

- Users may not understand VPN technology
- Lack of apps’ vetting process

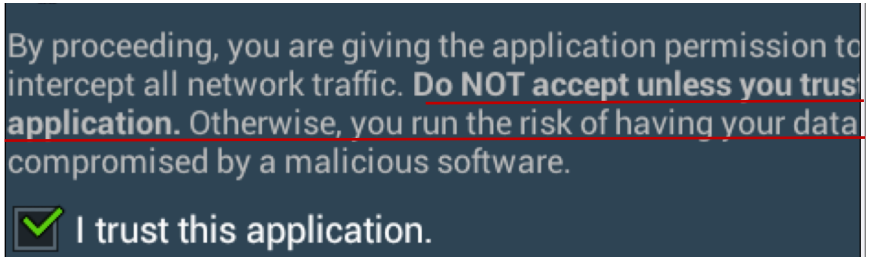


Attention

OpenVPN for Android attempts to create a VPN connection.

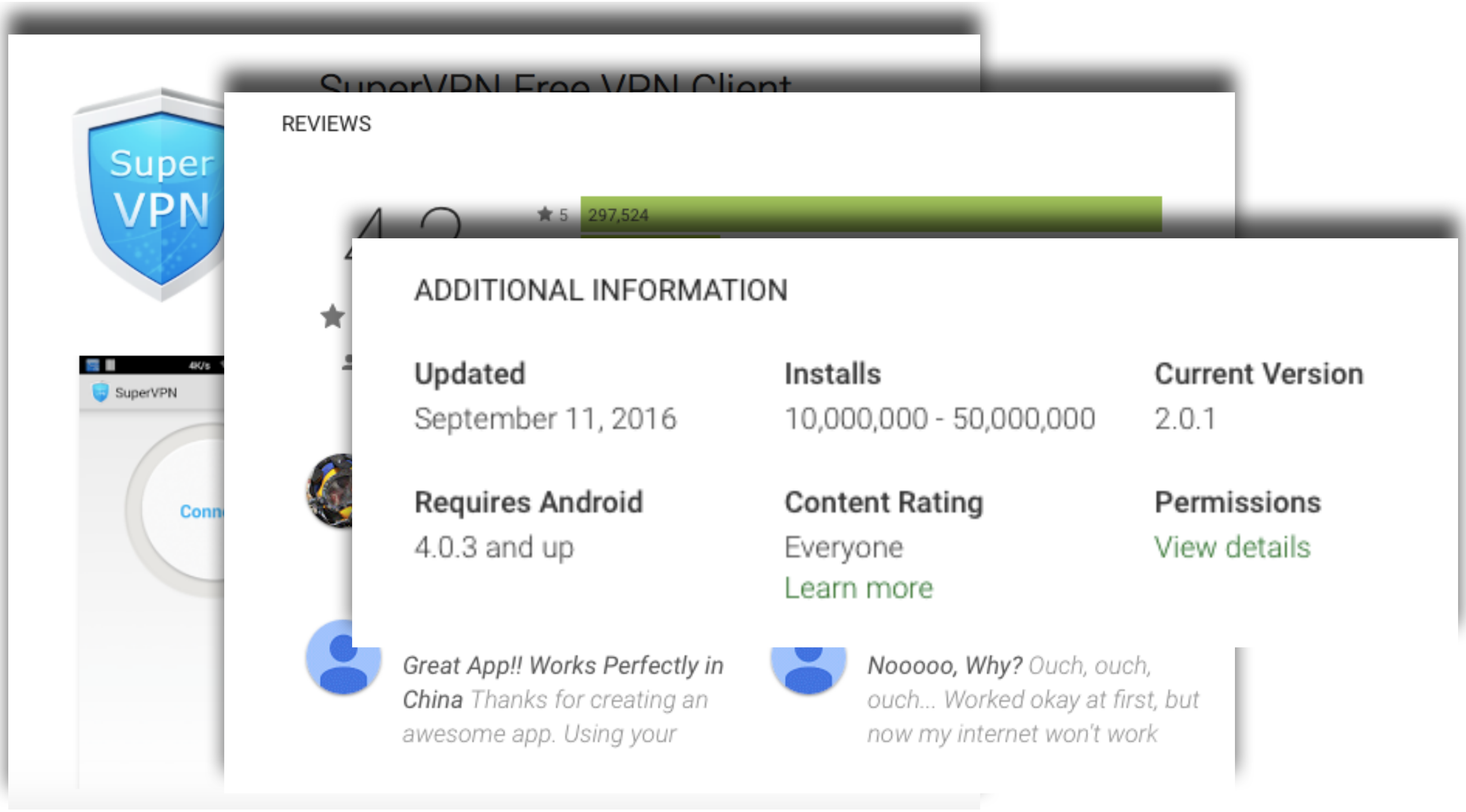
By proceeding, you are giving the application permission to intercept all network traffic. **Do NOT accept unless you trust the application.** Otherwise, you run the risk of having your data compromised by a malicious software.

☑ I trust this application.



By proceeding, you are giving the application permission to intercept all network traffic. **Do NOT accept unless you trust application.** Otherwise, you run the risk of having your data compromised by a malicious software.

☑ I trust this application.



ADDITIONAL INFORMATION

Updated	Installs	Current Version
September 11, 2016	10,000,000 - 50,000,000	2.0.1
Requires Android	**Content Rating**	**Permissions**
4.0.3 and up	Everyone Learn more	View details

Great App!! Works Perfectly in China *Thanks for creating an awesome app. Using your*

Nooooo, Why? *Ouch, ouch, ouch... Worked okay at first, but now my internet won't work*

Are VPN Android apps trustworthy?

Approach

1. Static Analysis

2. Network Measurements

Some salient results

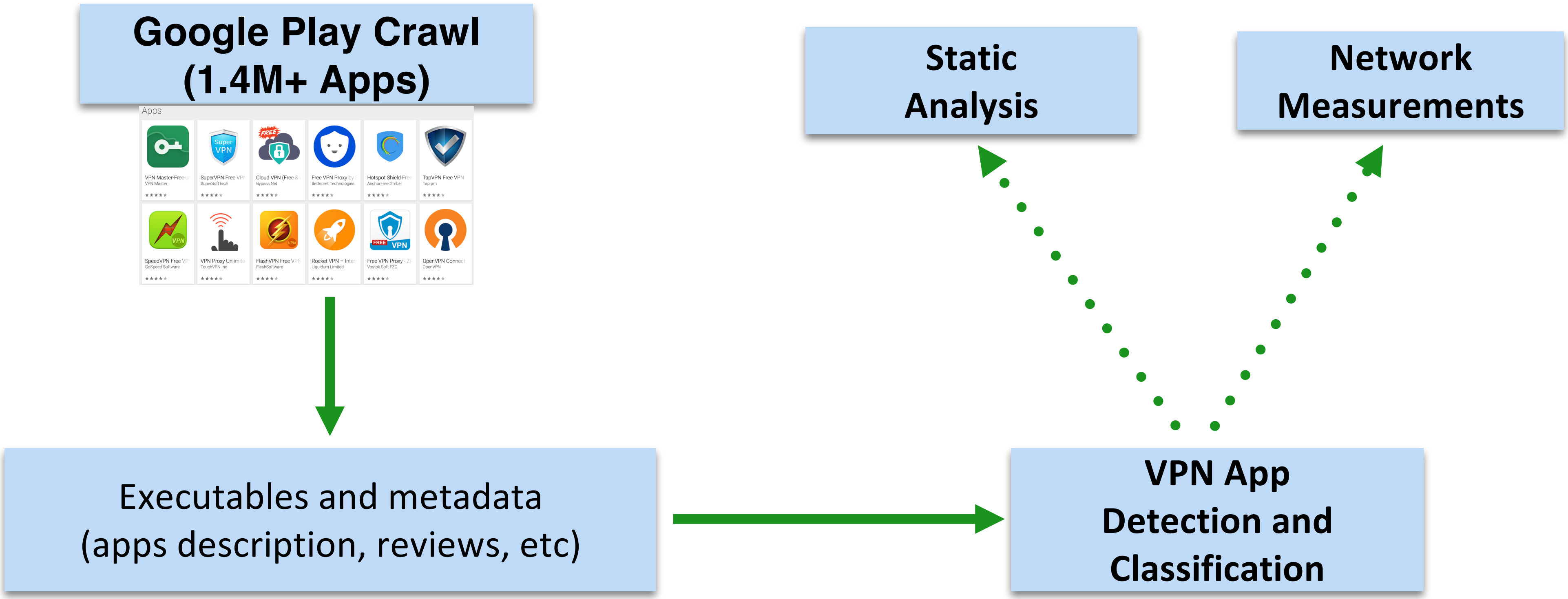
- Malware presence
- Traffic leak
- Javascript injection and TLS interception

2 apps inject JavaScript code
4 apps implement TLS interception

Agenda

- VPN App Detection and Methodology
- Passive Analysis
- Network Measurements
- Summary
- Developer’s feedback

Methodology



Google Play Crawl (1.4M+ Apps)

Executables and metadata (apps description, reviews, etc)

VPN App Detection and Classification

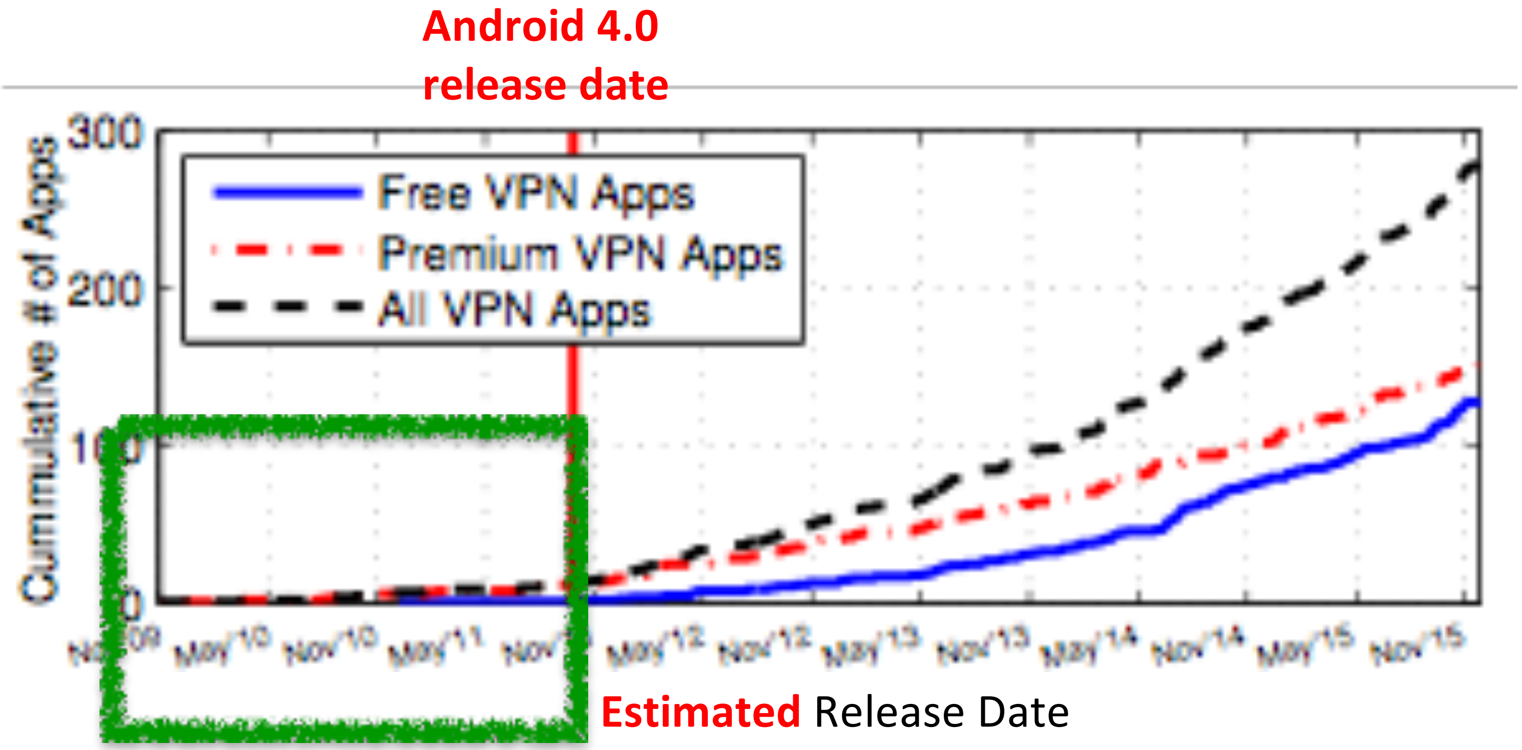
Static Analysis

Network Measurements

Identified VPN App

App Category	# of apps found (N = 283)
Free VPN apps with Free services	130
Free VPN apps with Premium services	153

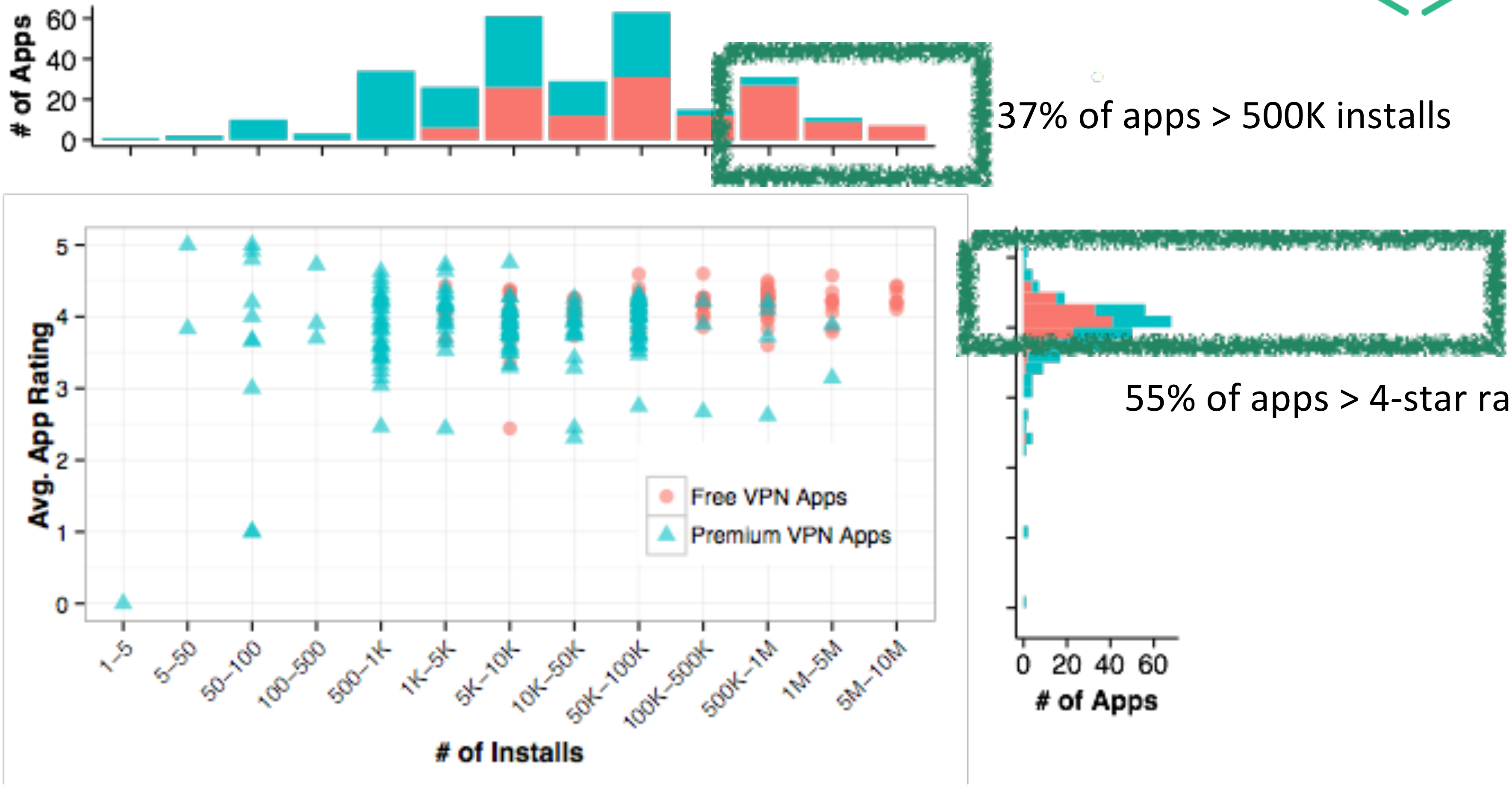
Analyzed VPN Apps - Evolution



Android 4.0 release date

Estimated Release Date

User installs and ratings



37% of apps > 500K installs

55% of apps > 4-star rating

Static Analysis

67% of Android VPN apps claim privacy and security enhancement features

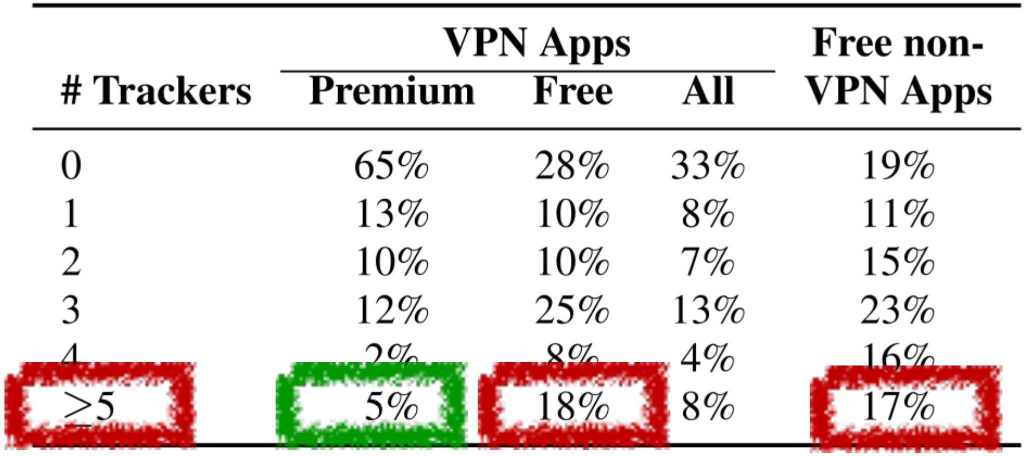
Access to Sensitive Data and Resources

- 82% of the VPN apps request sensitive permissions
  - READ_LOGS (14%)
  - READ_SMS (6%)
  - READ_CONTACTS (6%)
  - WRITE_SMS (4%)

Limitation: is the use of those permissions legitimate?

3rd-party Tracking Libraries

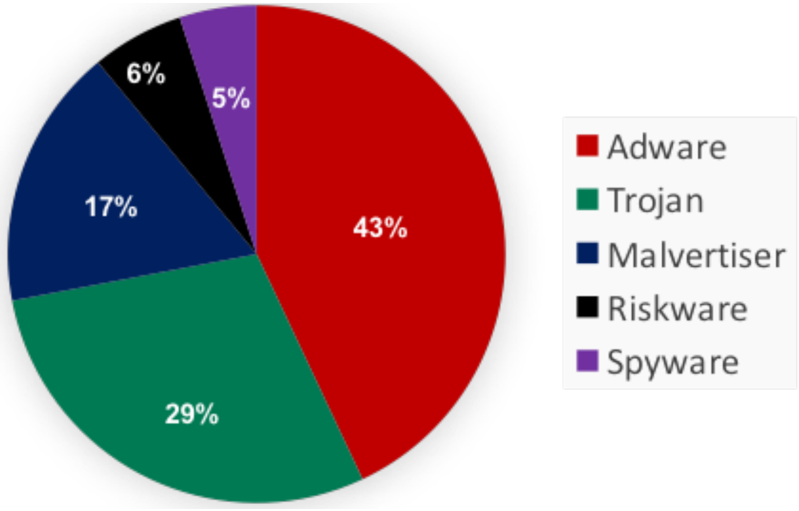
- 67% of VPN apps include 3rd-party tracking libraries

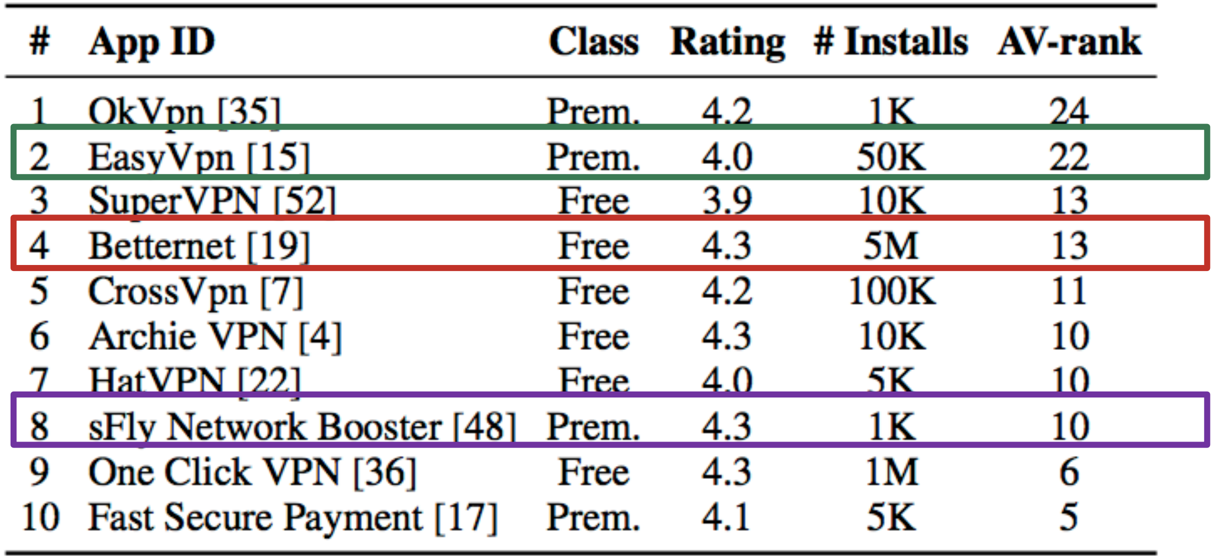


# Trackers	VPN Apps			Free non-VPN Apps
	Premium	Free	All	
0	65%	28%	33%	19%
1	13%	10%	8%	11%
2	10%	10%	7%	15%
3	12%	25%	13%	23%
4	2%	8%	4%	16%
≥5	5%	18%	8%	17%

Malware Presence

- Scanner: VirusTotal aggregator
- **AV-rank:** number of AV tools reporting malware
- 38% of VPN apps contain malware with 4% have AV-rank ≧ 5

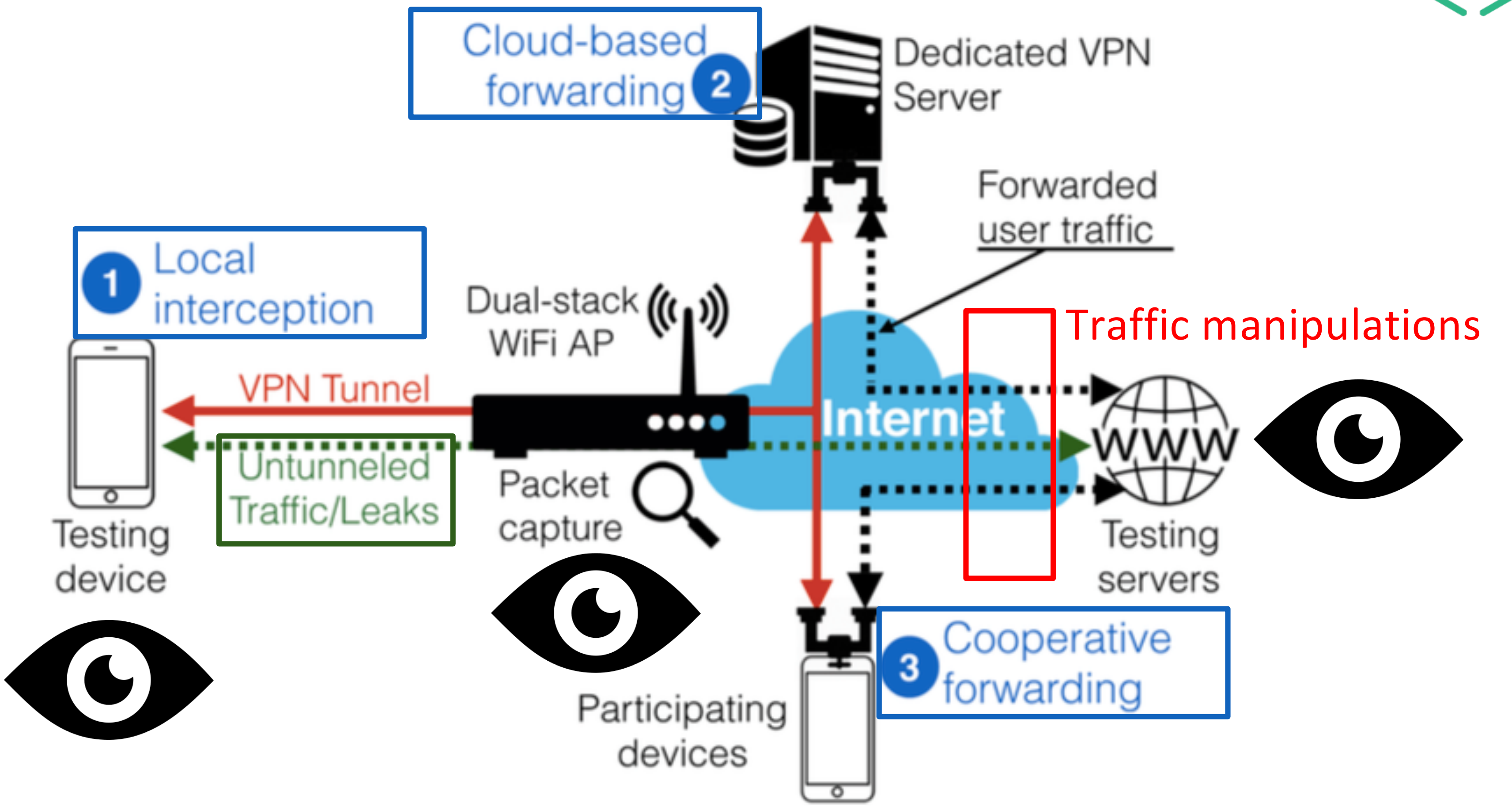




#	App ID	Class	Rating	# Installs	AV-rank
1	OkVpn [35]	Prem.	4.2	1K	24
2	EasyVpn [15]	Prem.	4.0	50K	22
3	SuperVPN [52]	Free	3.9	10K	13
4	Betternet [19]	Free	4.3	5M	13
5	CrossVpn [7]	Free	4.2	100K	11
6	Archie VPN [4]	Free	4.3	10K	10
7	HatVPN [22]	Free	4.0	5K	10
8	sFly Network Booster [48]	Prem.	4.3	1K	10
9	One Click VPN [36]	Free	4.3	1M	6
10	Fast Secure Payment [17]	Prem.	4.1	5K	5

Network Measurements

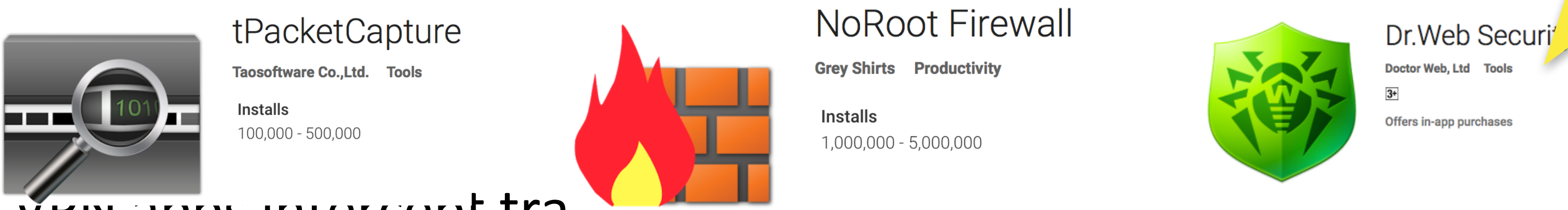
Testbed


Cloud-based forwarding 2
Dedicated VPN Server
Forwarded user traffic
1 Local interception
Dual-stack WiFi AP
Traffic manipulations
VPN Tunnel
Internet
WWW
Untunneled Traffic/Leaks
Packet capture
Testing device
Testing servers
Participating devices
3 Cooperative forwarding

Forwarding models

- Tested manually each vantage point reported in the app
- 18% of apps do not inform about the terminating end-point

1lt.su

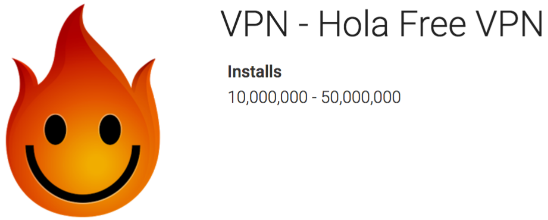


tPacketCapture
Taosoftware Co.,Ltd. Tools
Installs
100,000 - 500,000

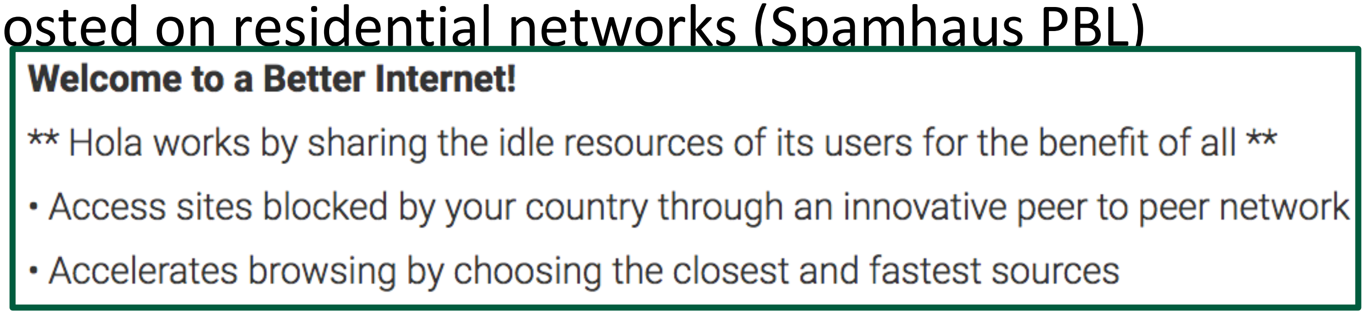
NoRoot Firewall
Grey Shirts Productivity
Installs
1,000,000 - 5,000,000

Dr.Web Securi
Doctor Web, Ltd Tools
3+
Offers in-app purchases

- 4% of VPN apps intercept traffic on localhost
- 16% use vantage points hosted on residential networks (Spamhaus PBL)



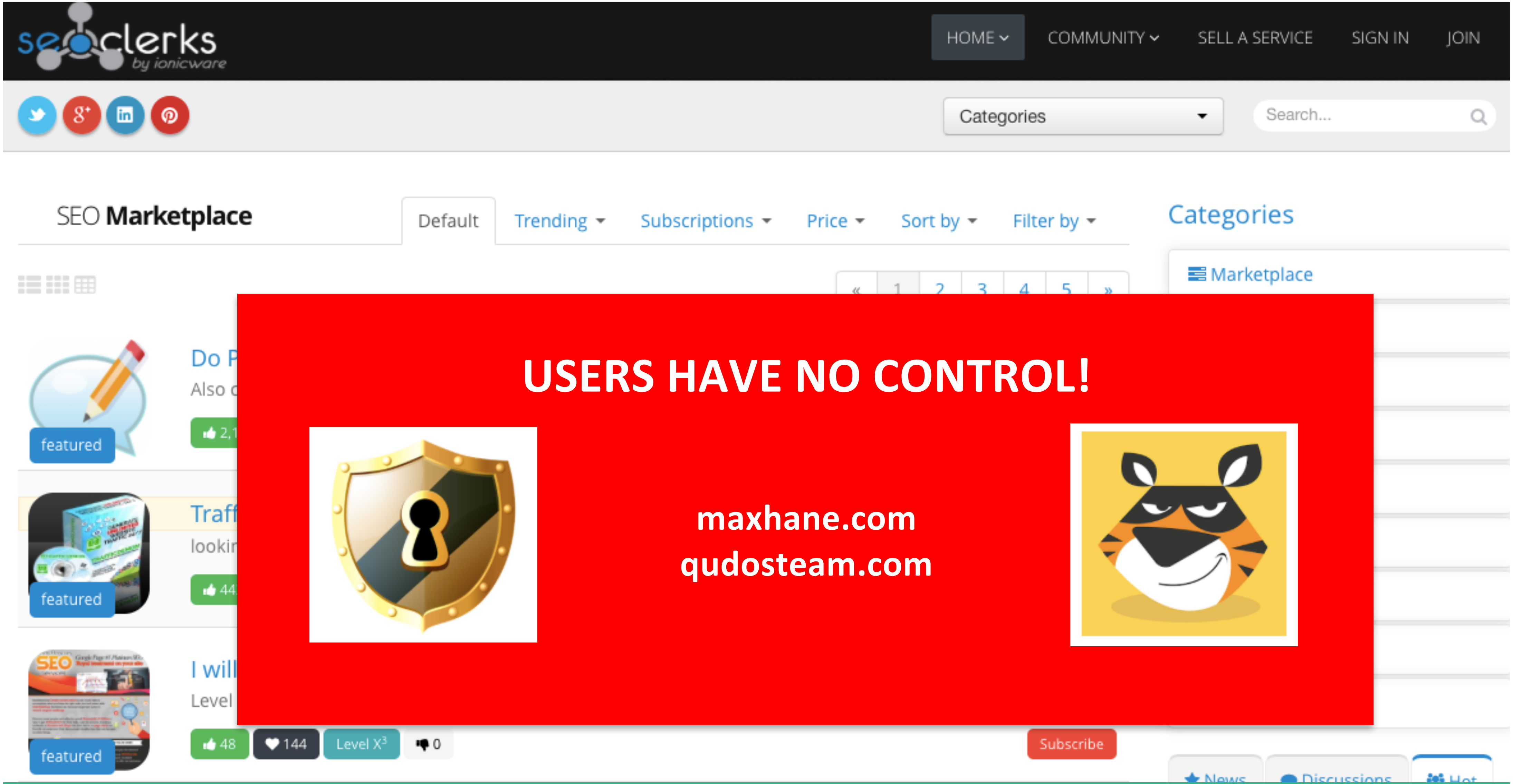
VPN - Hola Free VPN
Installs
10,000,000 - 50,000,000



Welcome to a Better Internet!

** Hola works by sharing the idle resources of its users for the benefit of all **

- Access sites blocked by your country through an innovative peer to peer network
- Accelerates browsing by choosing the closest and fastest sources



USERS HAVE NO CONTROL!

maxhane.com

qudosteam.com

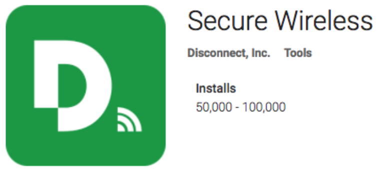
DNS and IPv6 Leakages

- 18% of apps do not use encrypted tunnels
- 84% of VPN apps leak IPv6 traffic
- 66% of VPN apps leaks DNS queries

Users can be potentially subject to in-path modification, profiling, redirection, and censorship.

Adblocking and JavaScript Injection

- DOM-based analysis
- Top 30 Alexa sites, reference website and seven e-commerce sites

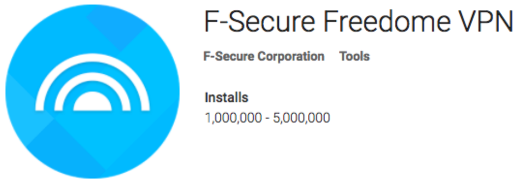


Secure Wireless

Disconnect, Inc. Tools

Installs

50,000 - 100,000

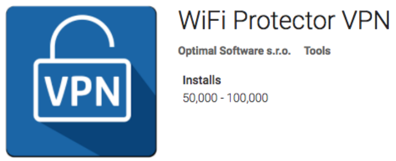


F-Secure Freedome VPN

F-Secure Corporation Tools

Installs

1,000,000 - 5,000,000

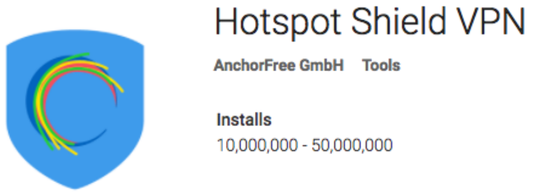


WiFi Protector VPN

Optimal Software s.r.o. Tools

Installs

50,000 - 100,000



Hotspot Shield VPN

AnchorFree GmbH Tools

Installs

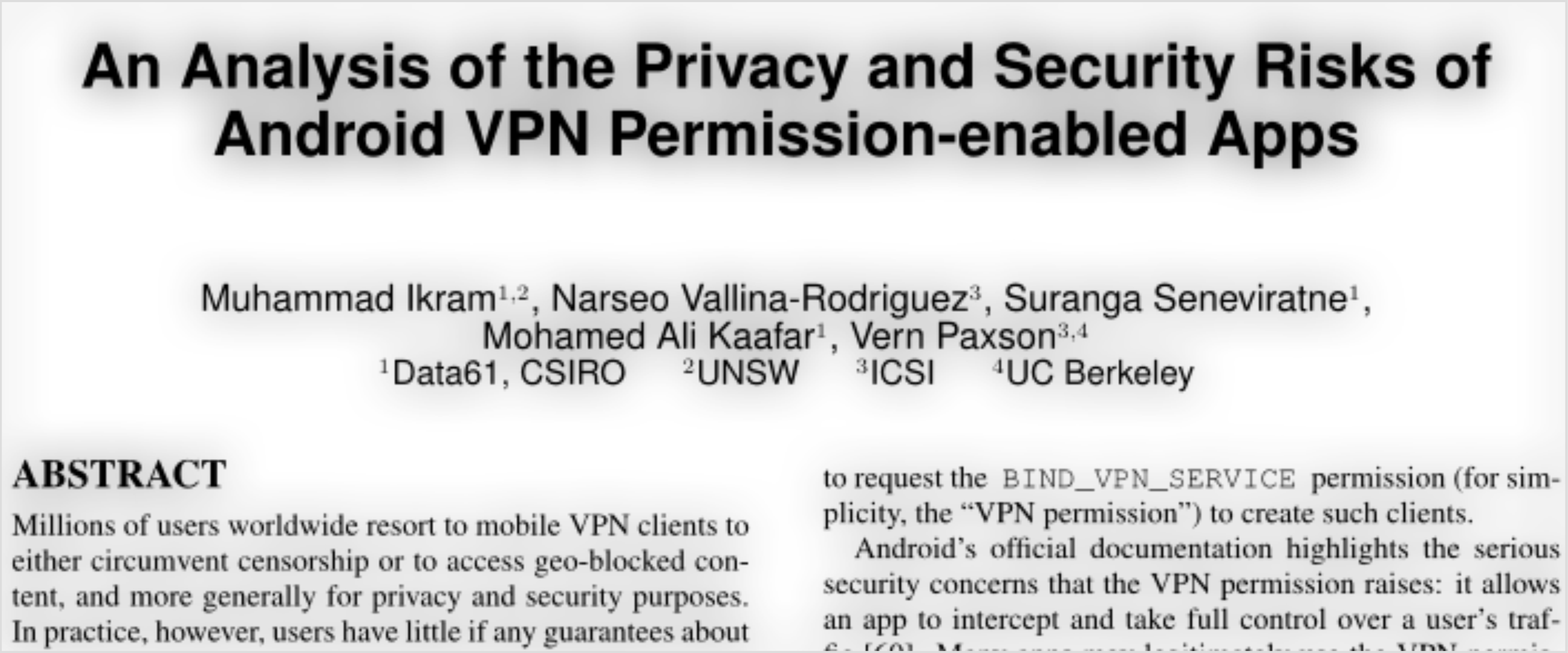
10,000,000 - 50,000,000

TLS Interception

- Analysed certificates from 60 websites/domains
- Apps compromise root store

Domain(port)	Neopard	DashVPN	DashNet	Packet Capture
amazon.com	❌	✅	❌	✅
gmail.com	✅	✅	✅	✅
orcart.facebook.com (8883)	✅	❌	❌	✅
bankofamerica.com	✅	✅	✅	✅
hsbc.com	❌	✅	❌	✅

More details:



An Analysis of the Privacy and Security Risks of Android VPN Permission-enabled Apps

Muhammad Ikram[1,2], Narseo Vallina-Rodriguez[3], Suranga Seneviratne[1],
Mohamed Ali Kaafar[1], Vern Paxson[3,4]
[1]Data61, CSIRO [2]UNSW [3]ICSI [4]UC Berkeley

ABSTRACT

Millions of users worldwide resort to mobile VPN clients to either circumvent censorship or to access geo-blocked content, and more generally for privacy and security purposes. In practice, however, users have little if any guarantees about

to request the BIND_VPN_SERVICE permission (for simplicity, the "VPN permission") to create such clients.

Android's official documentation highlights the serious security concerns that the VPN permission raises: it allows an app to intercept and take full control over a user's traffic [60]. Many apps may legitimately use the VPN permis-

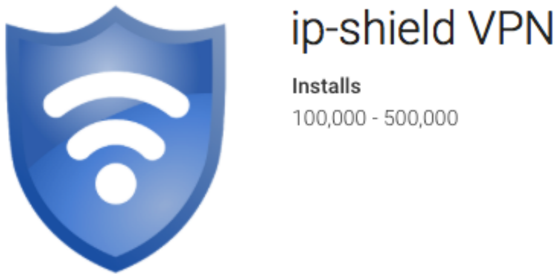
“And isn’t it ironic?”

- Do users care?
- Manually analysed negative reviews (4.5K) (1- and 2-Stars)
- < 1% of the negative reviews raised privacy and security concerns

Summary

- 38% of apps have malware presence
- 67% of apps have at least one third-party tracking library
- 66% of VPN apps have DNS leakages and 84% have IPv6 Leakages
- 2 VPN apps perform JS-injection for ads, tracking, and redirections
- 4 VPN apps perform TLS interception

Developer Feedback and Reactions



ip-shield VPN

Installs

100,000 - 500,000

"… Appflood [third-party library] was the best choice to monetize the app".

Now: ads- and tracking free app

WiFi Protector VPN

Optimal Software s.r.o. Tools

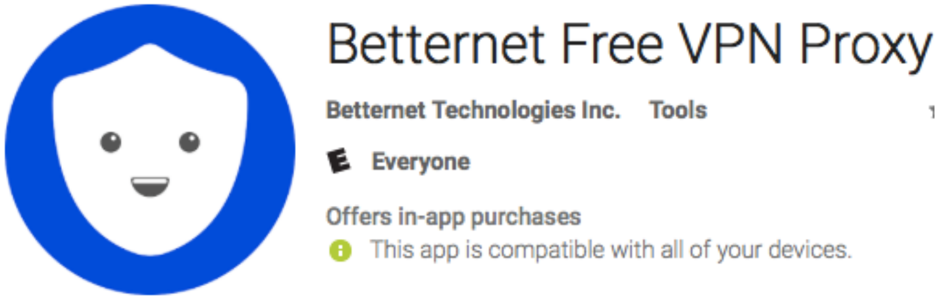
Installs

50,000 - 100,000

Confirmed JS-Injections for tracking users and showing their own advertisements

Now: status quo

Developer Feedback and Reactions



Betternet Free VPN Proxy

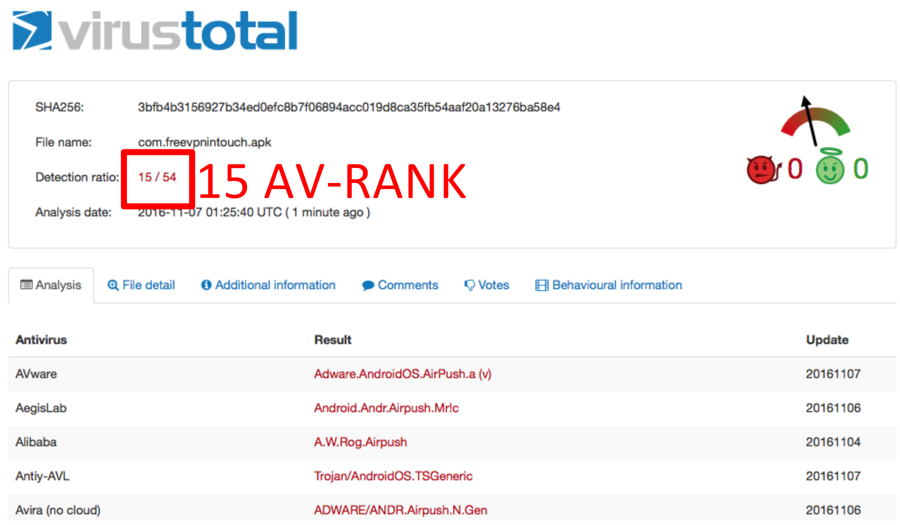
Betternet Technologies Inc. Tools

E Everyone

Offers in-app purchases

This app is compatible with all of your devices.

"… we will promise these problems never occur again."



virustotal

SHA256: 3bfb4b3156927b34ed0efc8b7f06894acc019d8ca35fb54aaf20a13276ba58e4

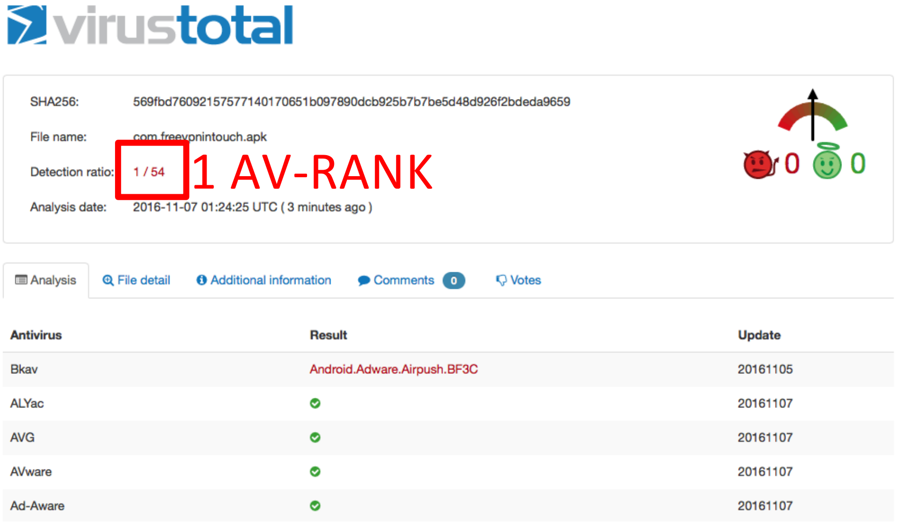
File name: com.freevpnintouch.apk

Detection ratio: 15 / 54 15 AV-RANK

Analysis date: 2016-11-07 01:25:40 UTC (1 minute ago)

Antivirus	Result	Update
AVware	Adware.AndroidOS.AirPush.a (v)	20161107
AegisLab	Android.Andr.Airpush.Mr!c	20161106
Alibaba	A.W.Rog.Airpush	20161104
Antiy-AVL	Trojan/AndroidOS.TSGeneric	20161107
Avira (no cloud)	ADWARE/ANDR.Airpush.N.Gen	20161106

November 2015



virustotal

SHA256: 569fbd76092157577140170651b097890dcb925b7b7be5d48d926f2bdeda9659

File name: com.freevpnintouch.apk

Detection ratio: 1 / 54 1 AV-RANK

Analysis date: 2016-11-07 01:24:25 UTC (3 minutes ago)

Antivirus	Result	Update
Bkav	Android.Adware.Airpush.BF3C	20161105
ALYac	✓	20161107
AVG	✓	20161107
AVware	✓	20161107
Ad-Aware	✓	20161107

October 2016

DATA
61

Thanks

Q&A

Muhammad Ikram
muhammad.ikram@data61.csiro.au

www.data61.csiro.au