DAVID WALKIEWICZ, MAIK MORGENSTERN
AVAR 2016

AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

Anti Virus Industry‘s Future Challenge:

PUA

ABOUT AV-TEST

PUA STANDS FOR …

Advertisement

Expectations

Reality

PUA and Security

Wikipedia …

Security

- **Install root certificate**
- Provide an **entry door for malware** (through exploits)
- Causing **issues on the system** – leading the user to remove /change the AV Software
- **Keylogger/KeyGenerator/PasswordReader** etc…
- ….

Basically is a potentially dangerous nuisance for the user and those poor admins fixing their parents device every weekend

EVERYBODY'S GOT TO EAT

Monetization

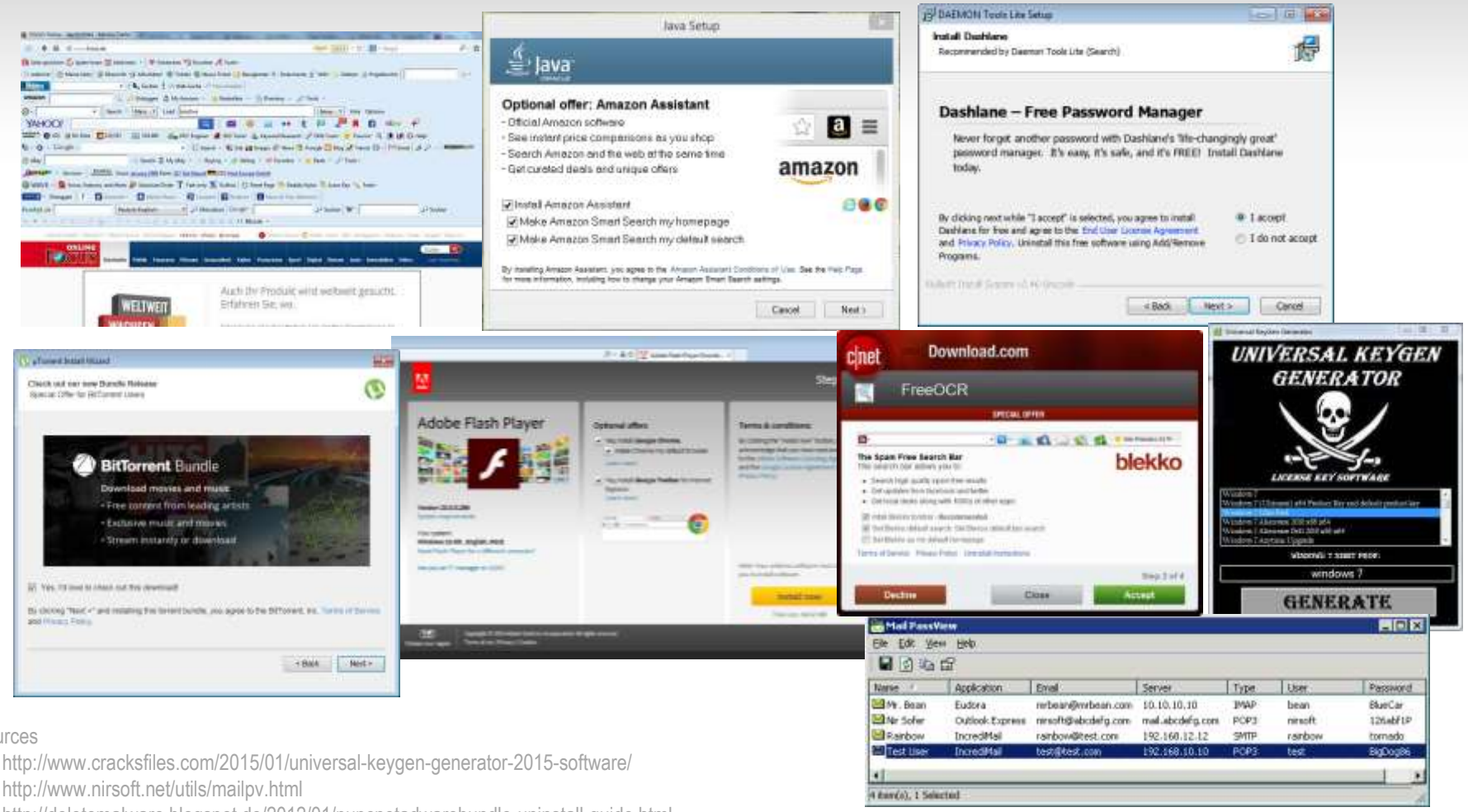
Non-objectionable means

- Share/Trialware
- SAAS or plain buying
- Advertisement on product webpage (Help, Forum etc.)
- Advertisement in products (App Stores apps)
- Non aggressive bundling

Questionable means

- Distribution through bundlers
- Information Harvesting
- Aggressive Advertisement

SOME PRETTY PICTURES – PUA BEHAVIOR



Sources

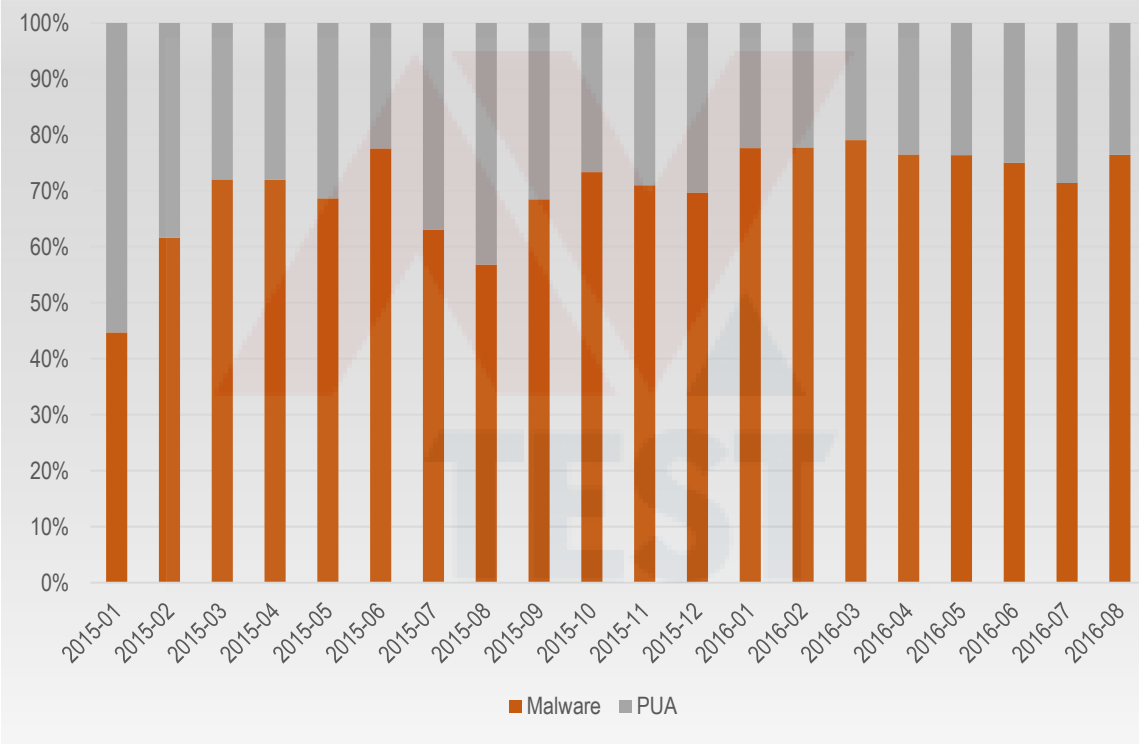
* http://www.cracksfiles.com/2015/01/universal-keygen-generator-2015-software/
* http://www.nirsoft.net/utils/mailpv.html
* http://deletemalware.blogspot.de/2012/01/pupcnetadwarebundle-uninstall-guide.html
* http://www.focus.de/digital/internet/anleitung-fuer-alle-browser-toolbar-ausversehen-installiert-so-werden-sie-die-leiste-wieder-los_id_4143166.html

DISTRIBUTION COMPARED TO MALWARE

Malware vs. PUA

10 million unique Files/Month

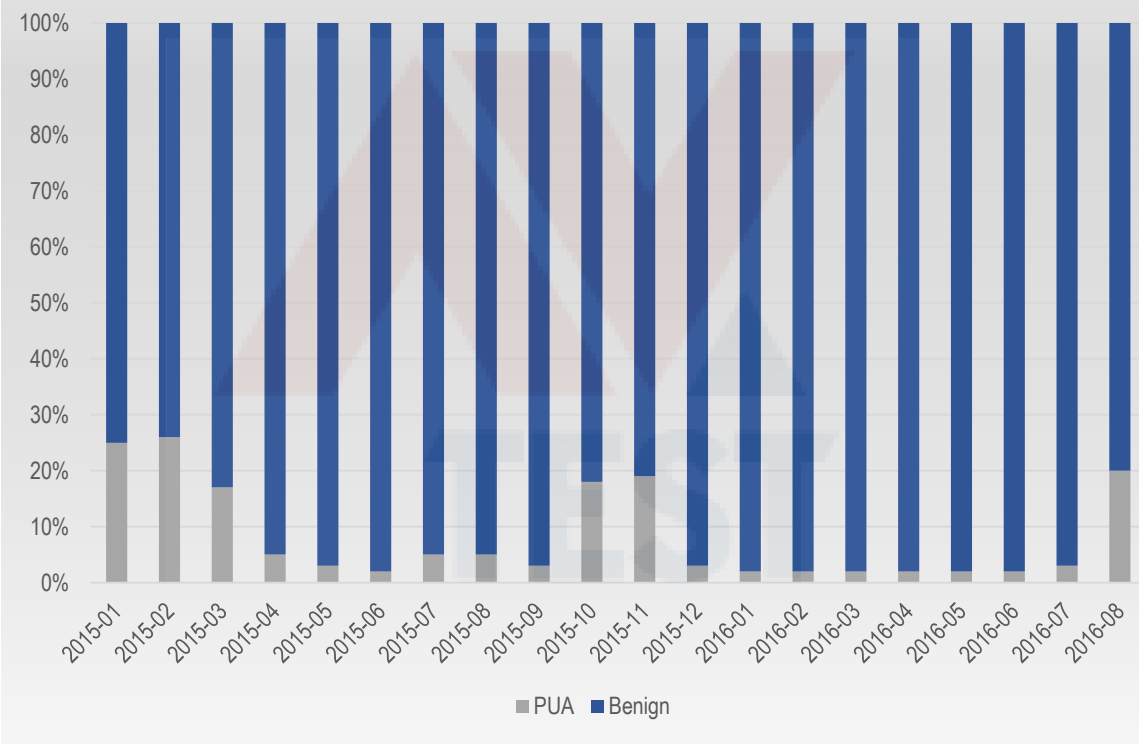
Windows, Linux, Android and Mac



“IN THE WILD” PUA VS BENIGN APPS, WINDOWS

Benign vs. PUA

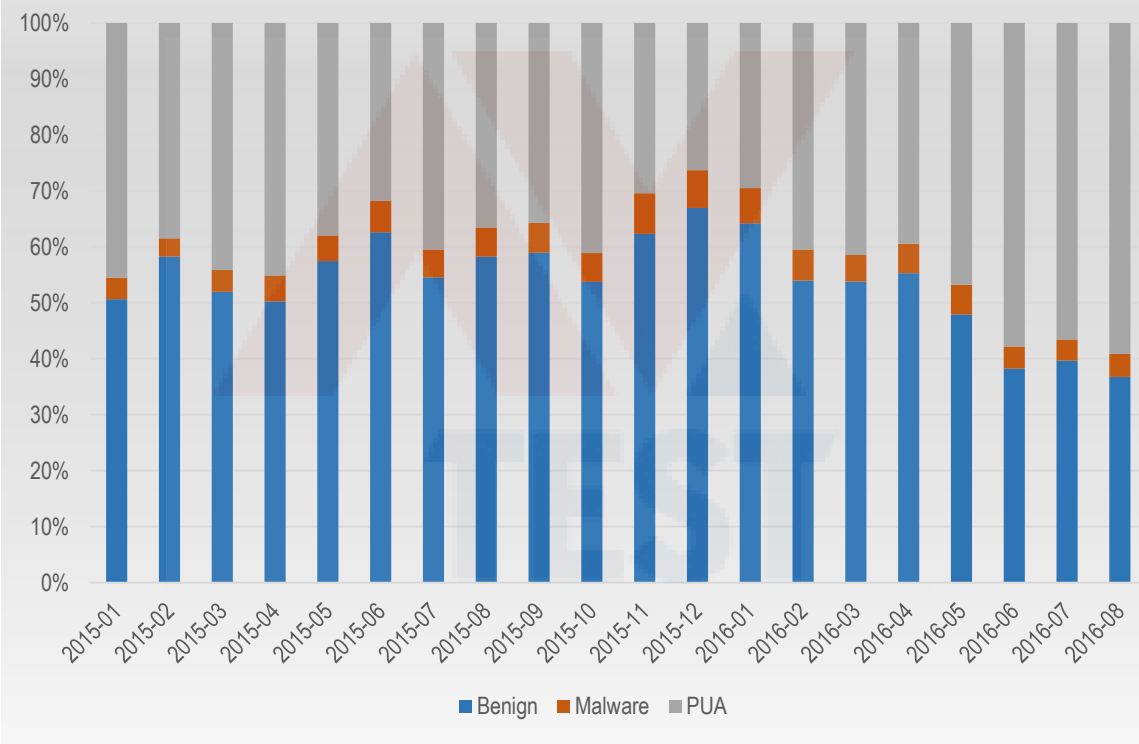
14.000 unique Installer/Month



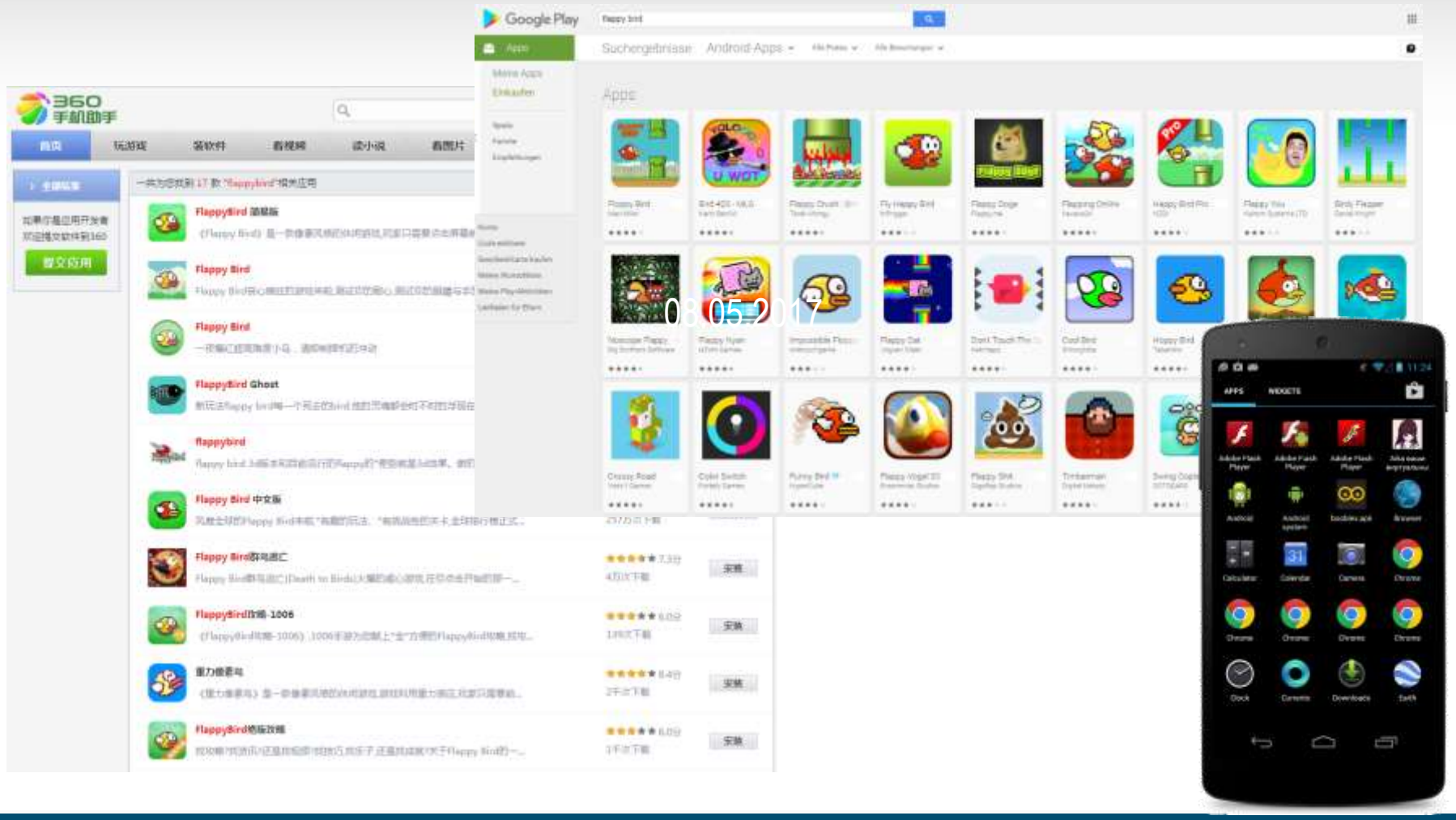
“IN THE WILD” PUA VS BENIGN APPS, ANDROID

Benign vs. PUA including Malware

20.000 unique APKs/Month

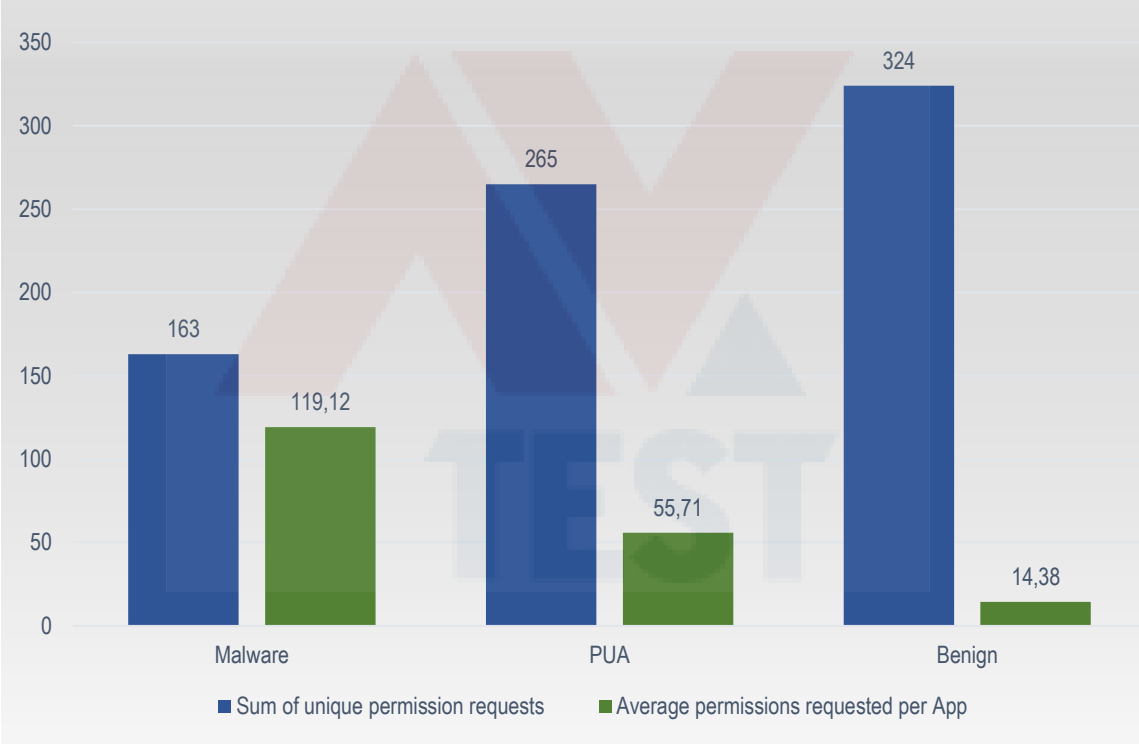


ISSUES WITH MONETIZATION STRATEGIES



PERMISSION REQUESTS ON ANDROID

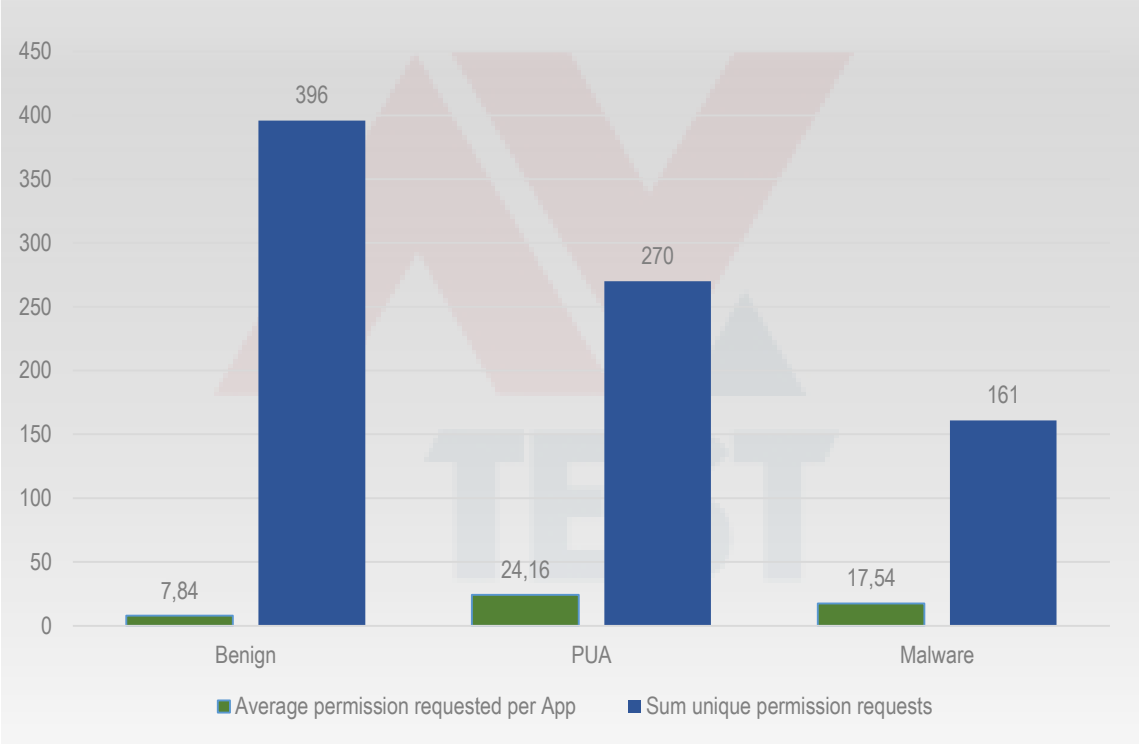
1.000 Malware,
600 PUA and
600 Benign
unique samples



July 2016

PERMISSION REQUESTS ON ANDROID

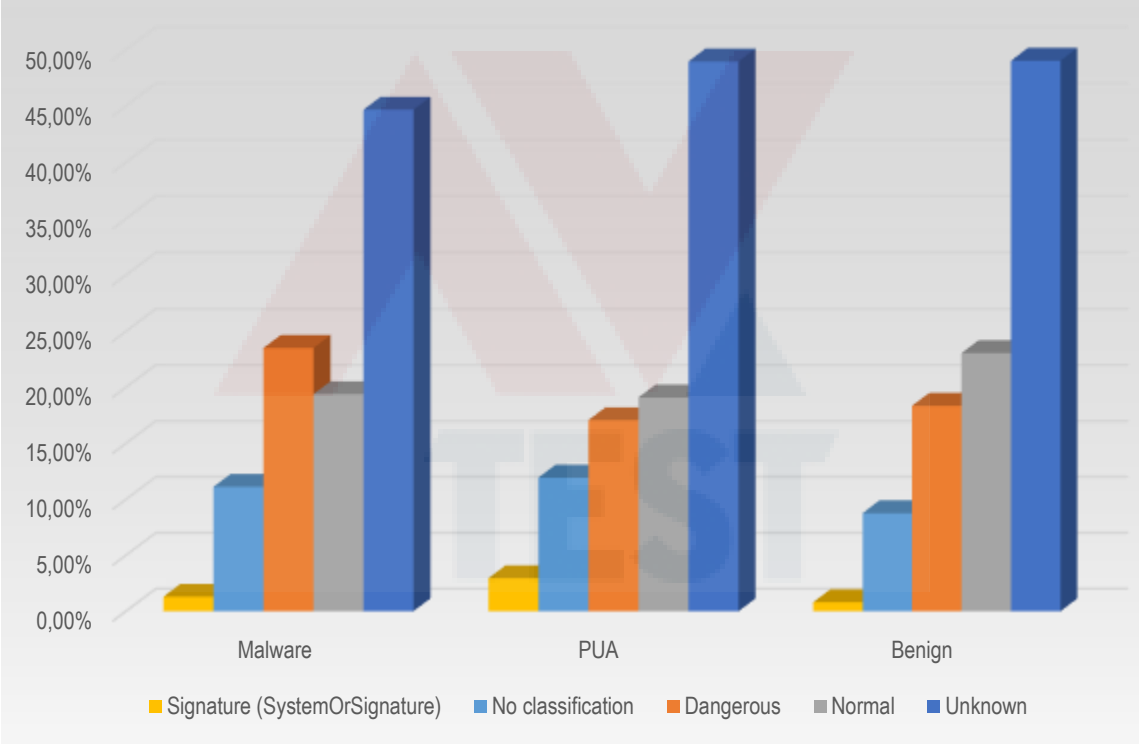
1.000 Malware,
600 PUA and
600 Benign
unique samples



July 2016

CLASSIFICATION OF REQUESTED PERMISSIONS

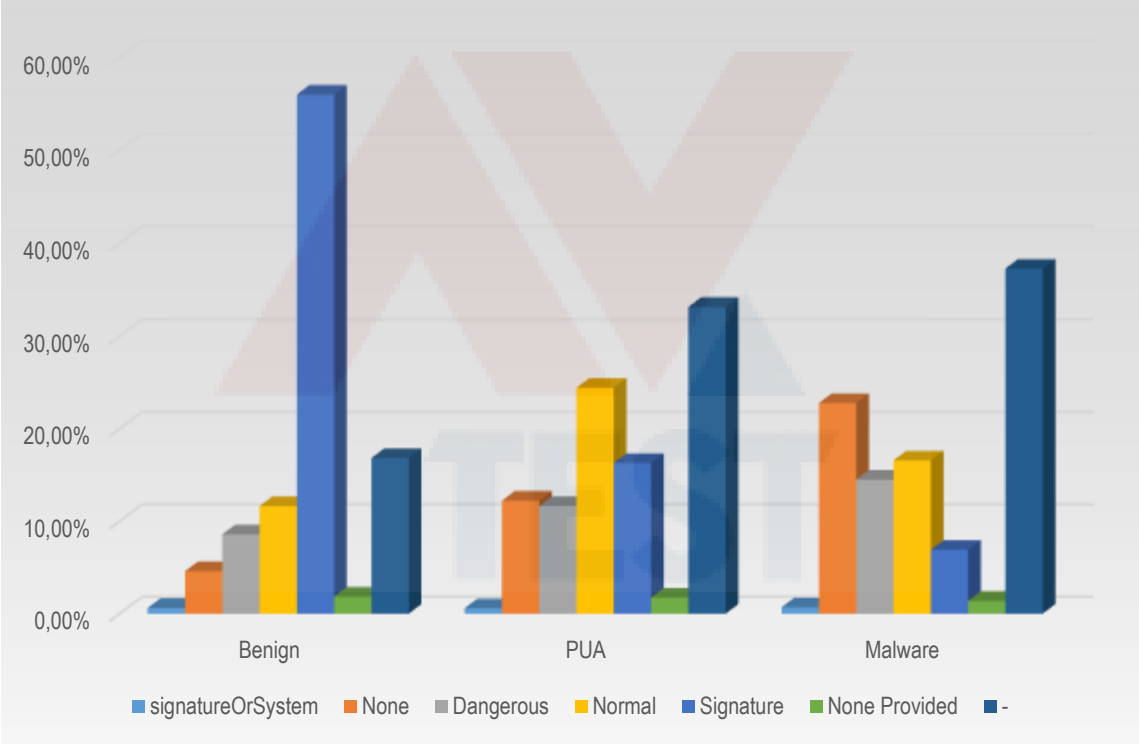
Permission classification provided by Google and Permissions set in Manifest



July 2016

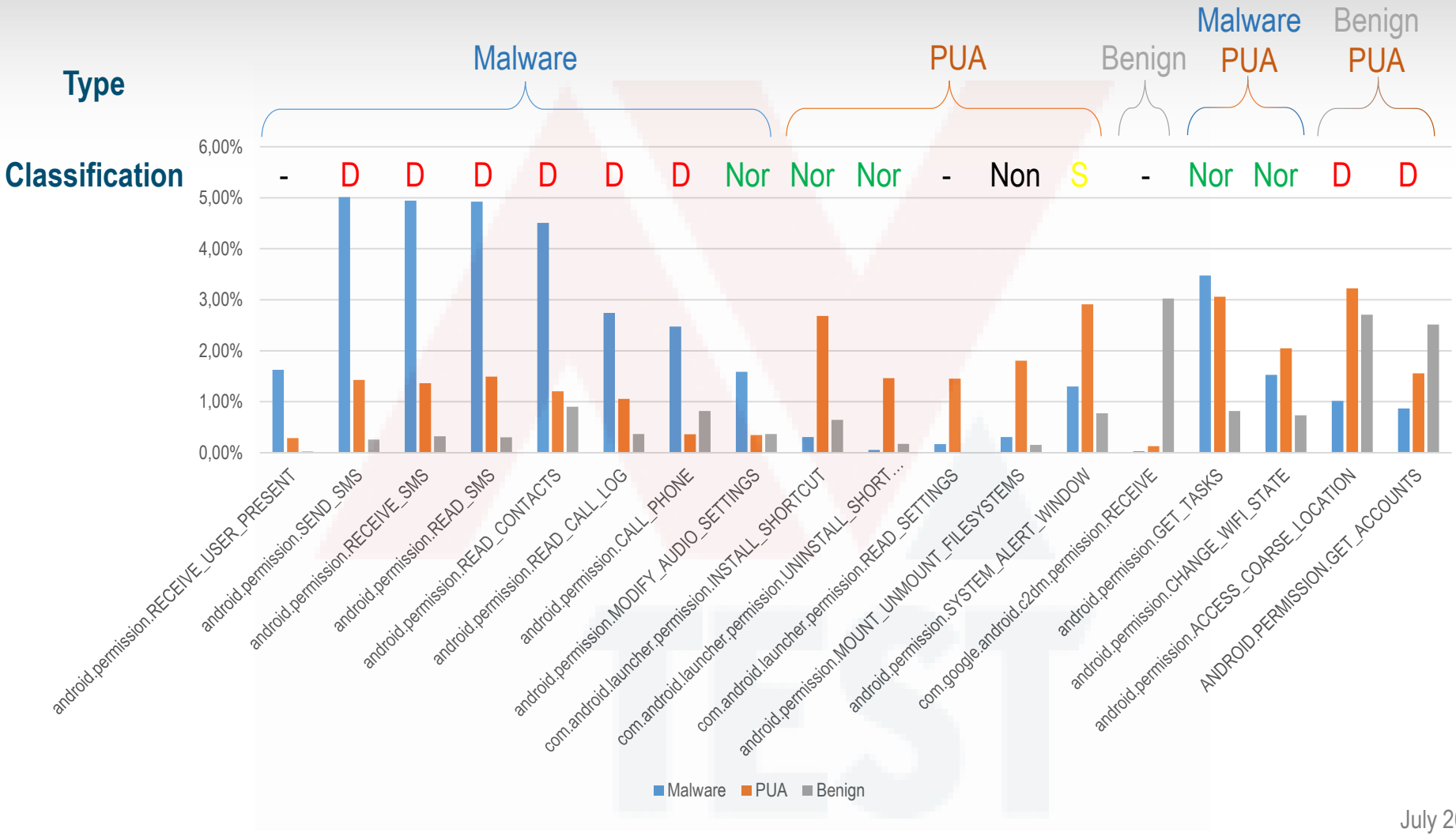
CLASSIFICATION OF REQUESTED PERMISSIONS

Permission classification provided by Google and Permissions set in Manifest



July 2016

CLASSIFICATION OF REQUESTED PERMISSIONS CONT.



July 2016

DATA TRANSMITTED, ANDROID AND WINDOWS

Android

	Benign	PUA
IMEI (International Mobile Station Equipment Identity)	0,00%	**27,56%**
Device id (unique device identifier)	0,00%	**2,95%**
Root (device rooted or not)	0,00%	**3,64%**
Agent (user agent of browser)	0,16%	**3,29%**
IP Dest (IP destination)	0,32%	**2,25%**
Mac (unique network adapter address)	2,23%	**10,57%**
Device Model	9,38%	**28,25%**
OS Version	7,00%	**15,42%**

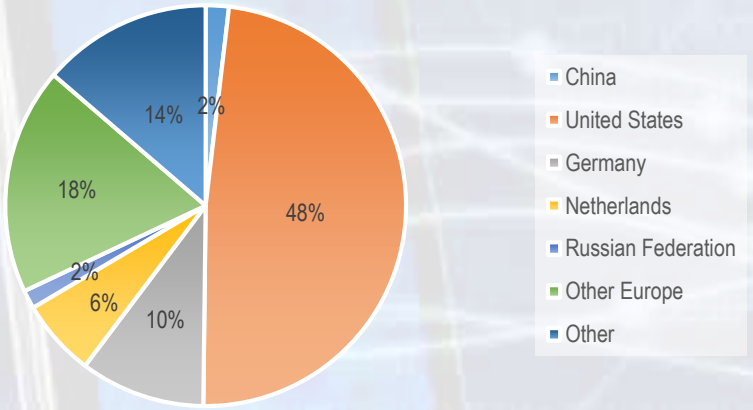
Windows

	Benign	PUA	Malware
Relevant transmitted PUA data			
Computer name	0,10%	**7,36%**	0,14%
Country	0,66%	**8,23%**	0,07%
City	0,00%	**1,25%**	0,00%
Relevant transmitted malware data			
Browser details	0,05%	1,25%	**13,16%**
Region	0,00%	1,37%	**4,46%**

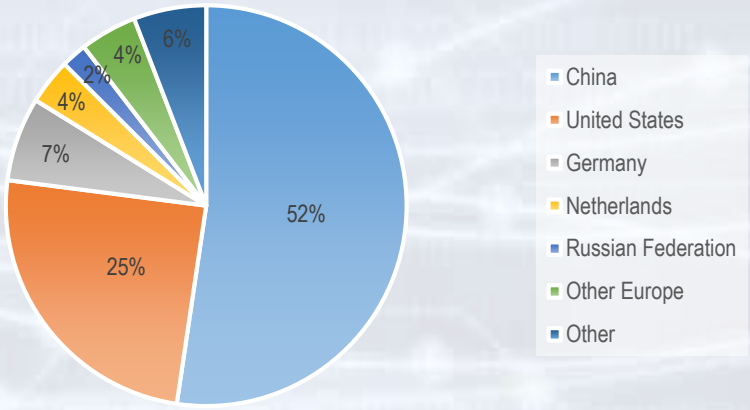
July 2016

DESTINATION OF DATA TRANSMITTED, ANDROID

Benign Traffic Destination



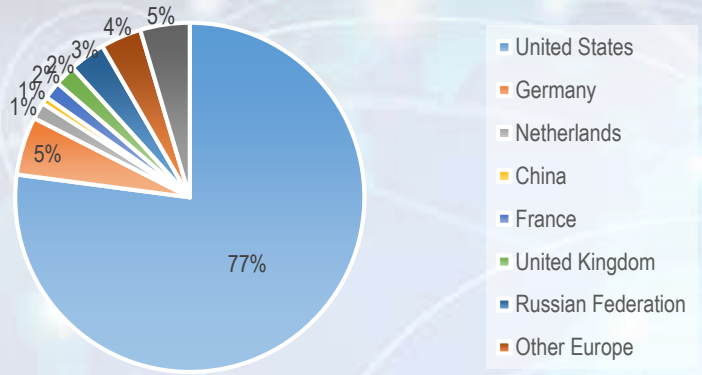
PUA Traffic Destination



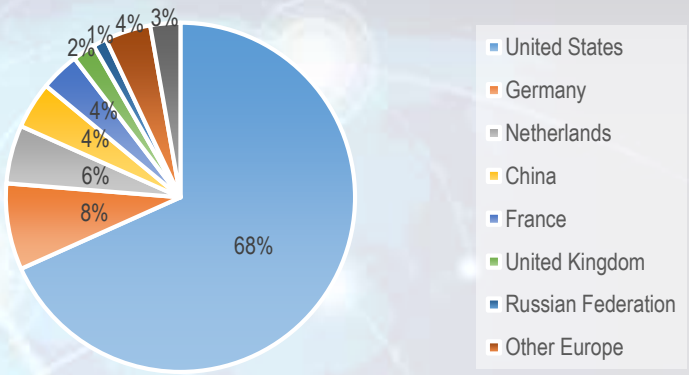
July 2016

DESTINATION OF DATA TRANSMITTED, WINDOWS

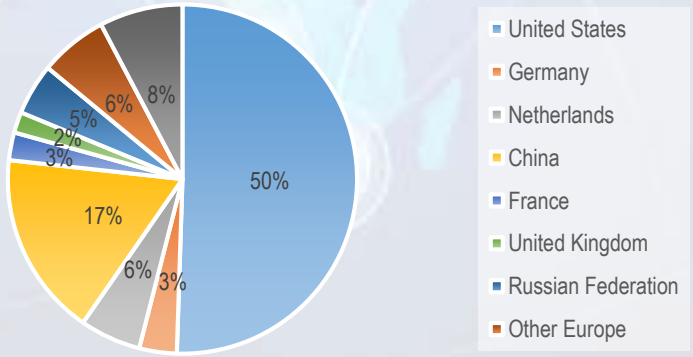
Benign Traffic Destination



PUA Traffic Destination



Malware Traffic Destination



July 2016

THREAT TO PRIVACY AND BUSINESS SECURITY

Where AVs fit in

Protection against malware and infections

Providing additional Security features like reputation of files and webpages, secure banking, file vaults, parental control etc.

Provide a hassle free usage of device by not slowing the computer and being mostly invisible

Protect Privacy

…

And provide protection against disruptive software

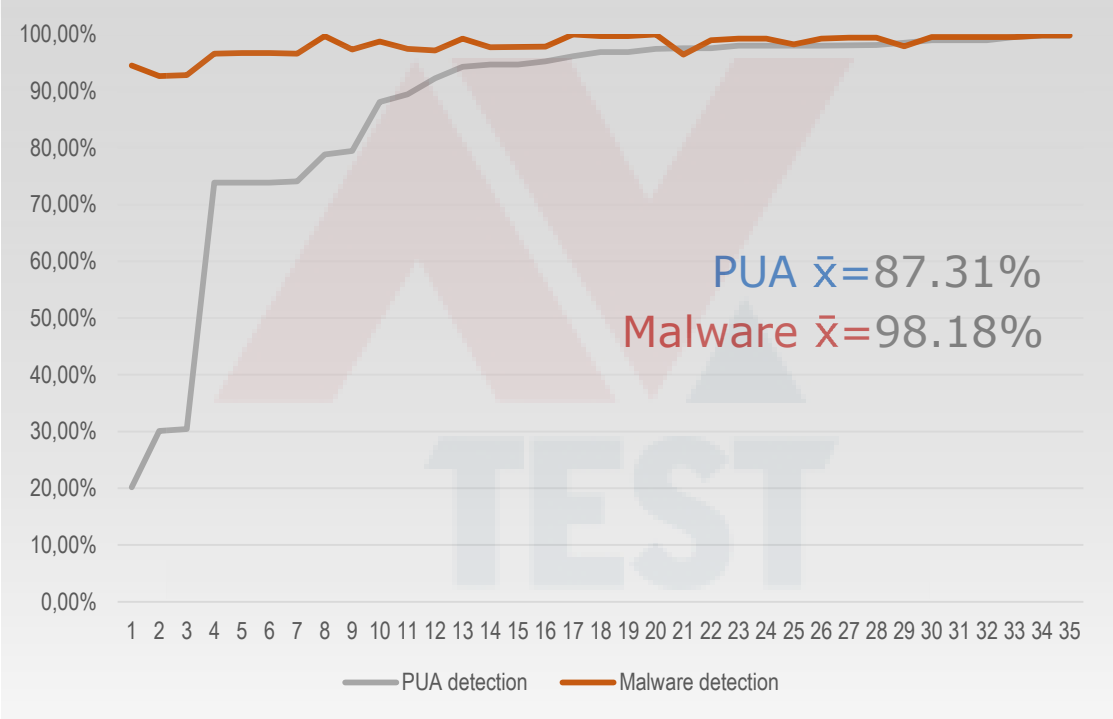
PUA DETECTION

	Windows	Android
PUA detection choice during Setup	03/35	1/22
In-App Option change PUA Settings (activated by default)	17/35	05/22
In-App Option change PUA Settings (deactivated by default)	04/35	04/22
PUA detection present but no option to change settings	08/35	10/22
No Option to detect PUA, low detection rate	03/35	02/22
Malware Average detection rate	**98,18%**	**99,63%**
PUA Average detection rate	**87,31%**	**93,98%**

July/August 2016

PUA VS MALWARE DETECTION RATE, WINDOWS

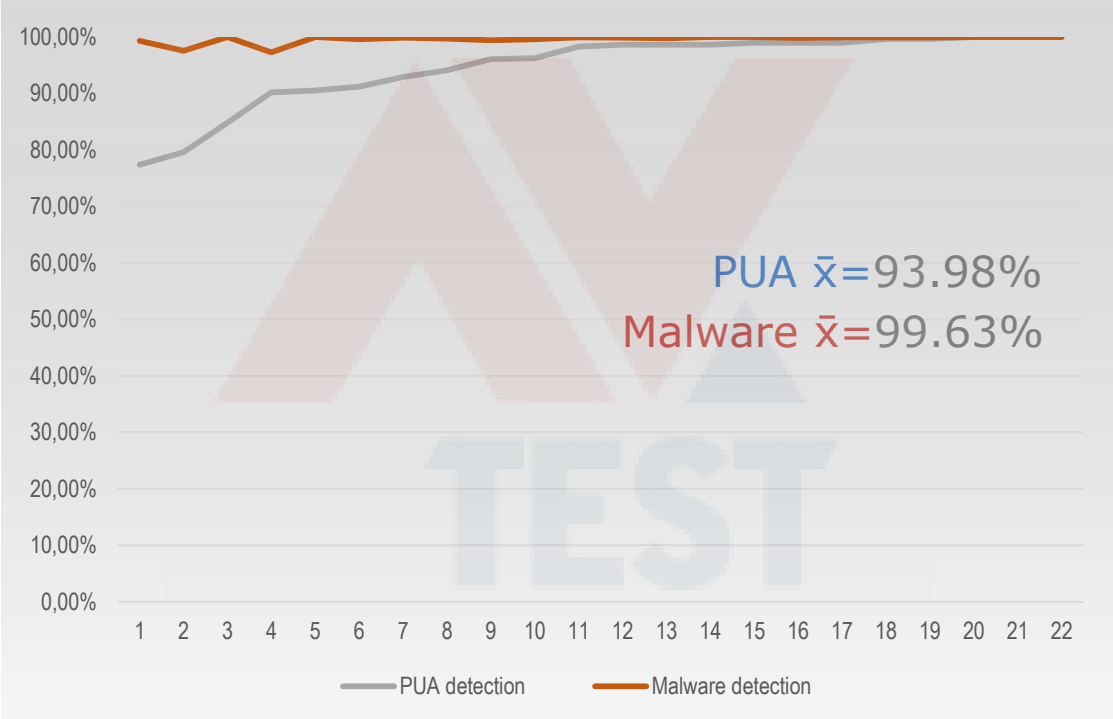
PUA vs. Malware detection rate per product (on-demand)



August 2016

PUA VS MALWARE DETECTION RATE, ANDROID

PUA vs. Malware detection rate per product



July 2016

CONCLUSION

PUA is a problem **as prevalent as Malware**, maybe more…

Users are **more likely to 'see' PUA** instead of Malware.

More **private data** saved **on digital/mobile devices.**

Data is targeted by everyone, governments, vendors, distributers.

Users expect AV to protect or at least warn them.

Even more focus must be put on protecting data on devices

@avtestorg (English) & @avtestde (German)

Follow us on facebook.com/avtestorg

Latest test results on https://www.av-test.org

Thank you for your attention!