DAVID WALKIEWICZ / MAIK MORGENSTERN

CARO Workshop 2016

PUA

DISTRIBUTION AND DETECTION

ABOUT AV-TEST

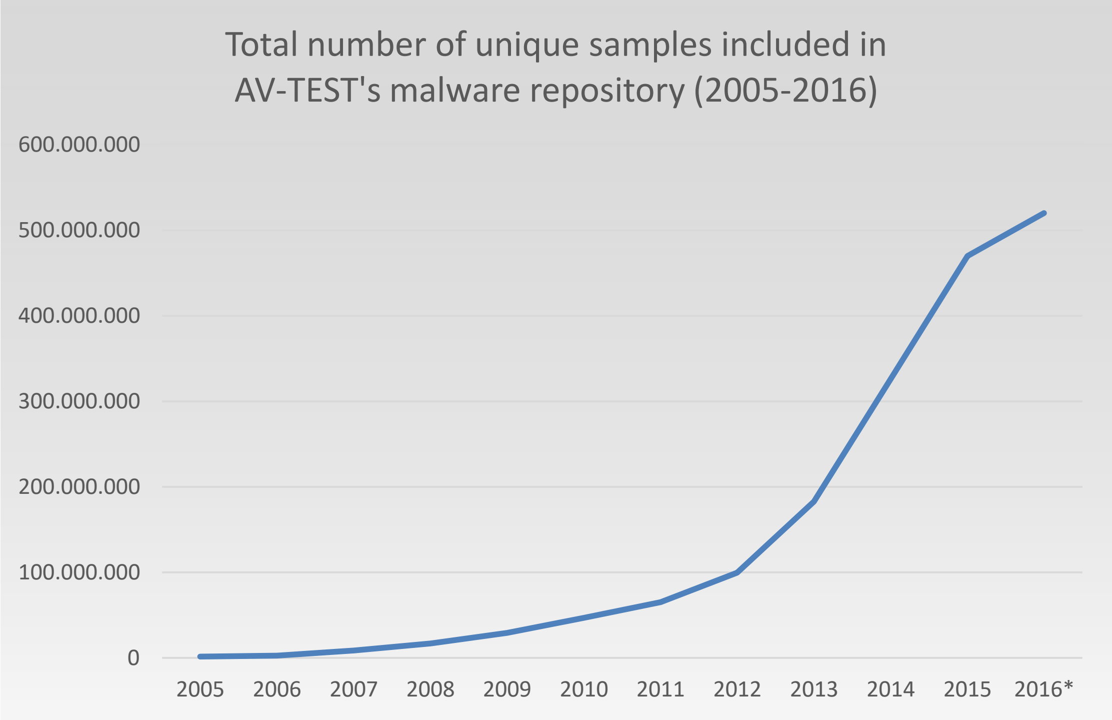
The AV-TEST Institute in Magdeburg

SOME STATISTICS FIRST

New scary numbers every year!

More Malware than ever before!

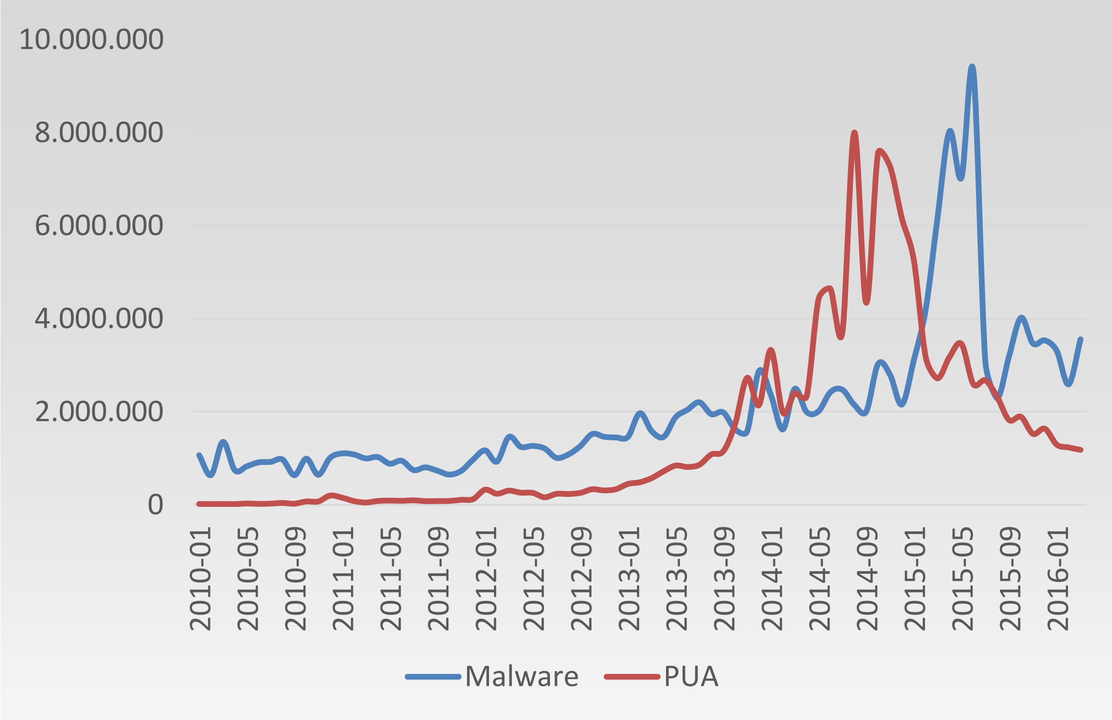
Just Malware?



SOME STATISTICS FIRST

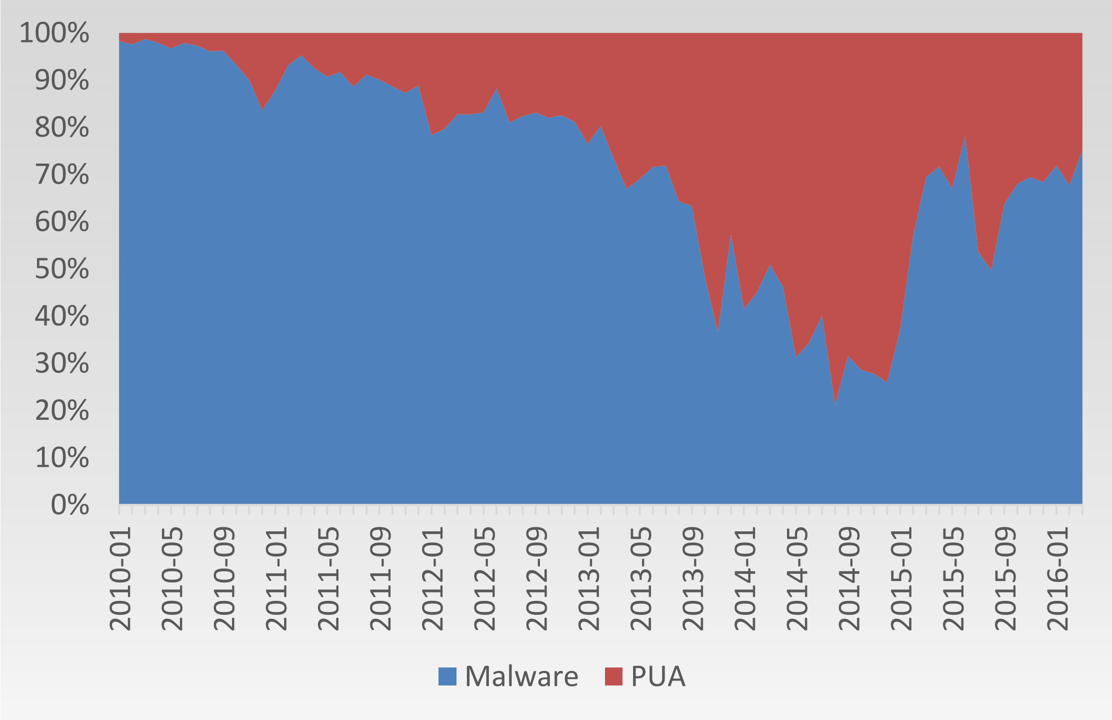
Development of Malware and PUA for Windows from 2010 to now

266 Million files received with at least 5 detections



SOME STATISTICS FIRST

Development of Malware and PUA for Windows from 2010 to now



57.77% classified as Malware

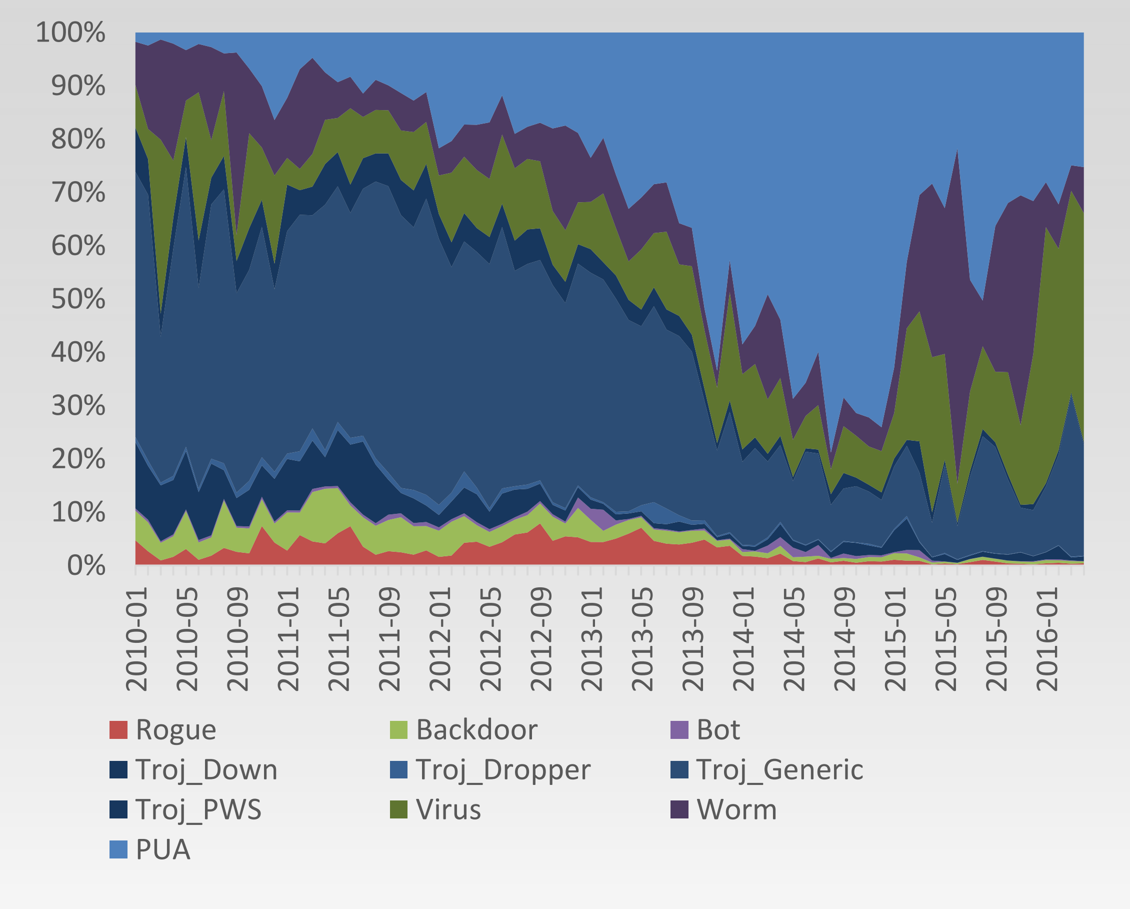
41.53% classified as PUA

SOME STATISTICS FIRST

Distribution of Malware and PUA

PUA by far the largest group with 110 Million files

Second biggest group is Trojans with with 66 Million files

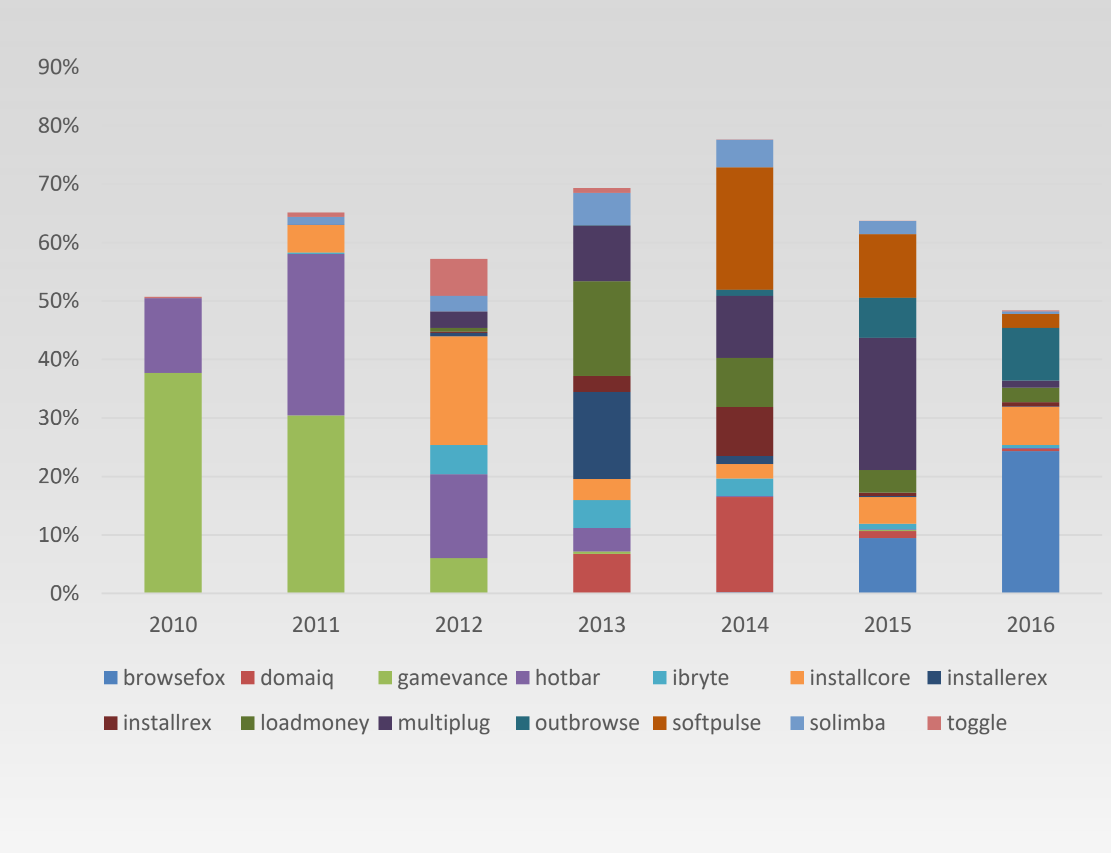


SOME STATISTICS FIRST

Prevalent PUA Families per year

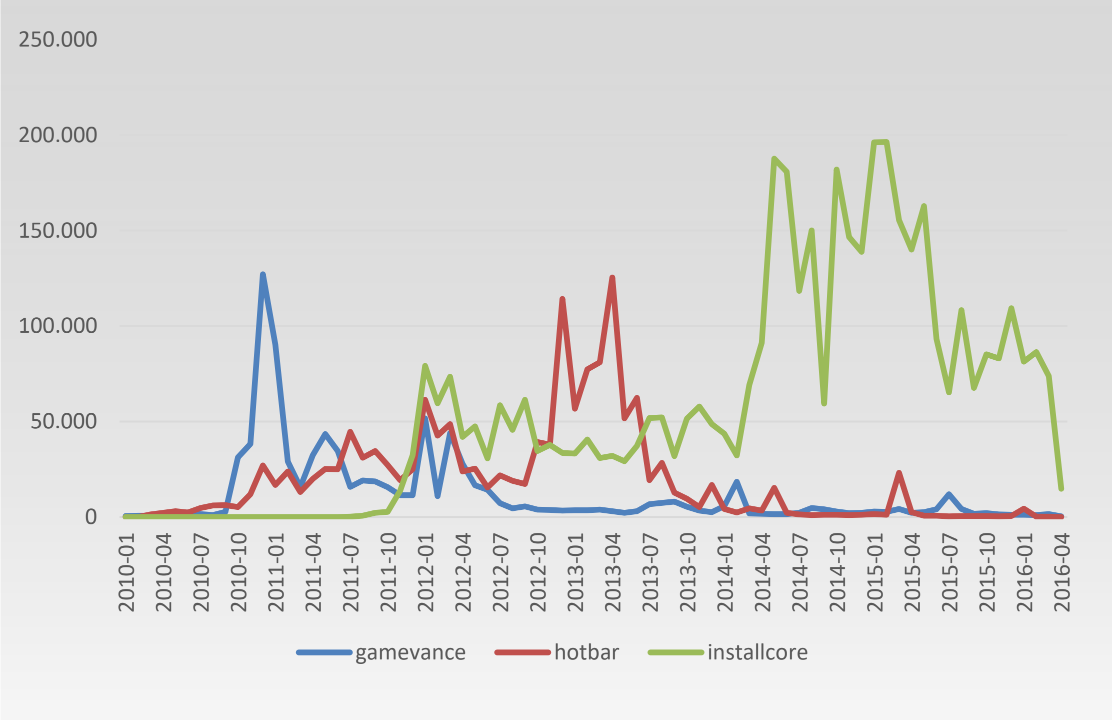
Families have their ups and downs

Number of prevalent families increased



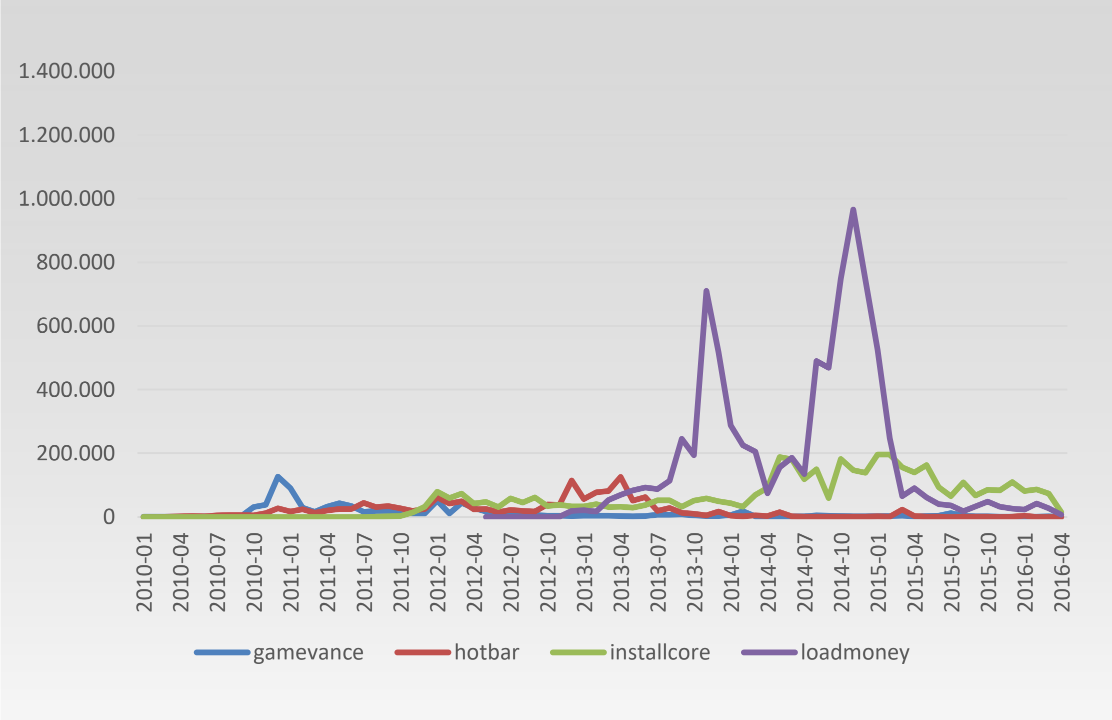
SOME STATISTICS FIRST

Prevalence and Distribution changed a lot during the years



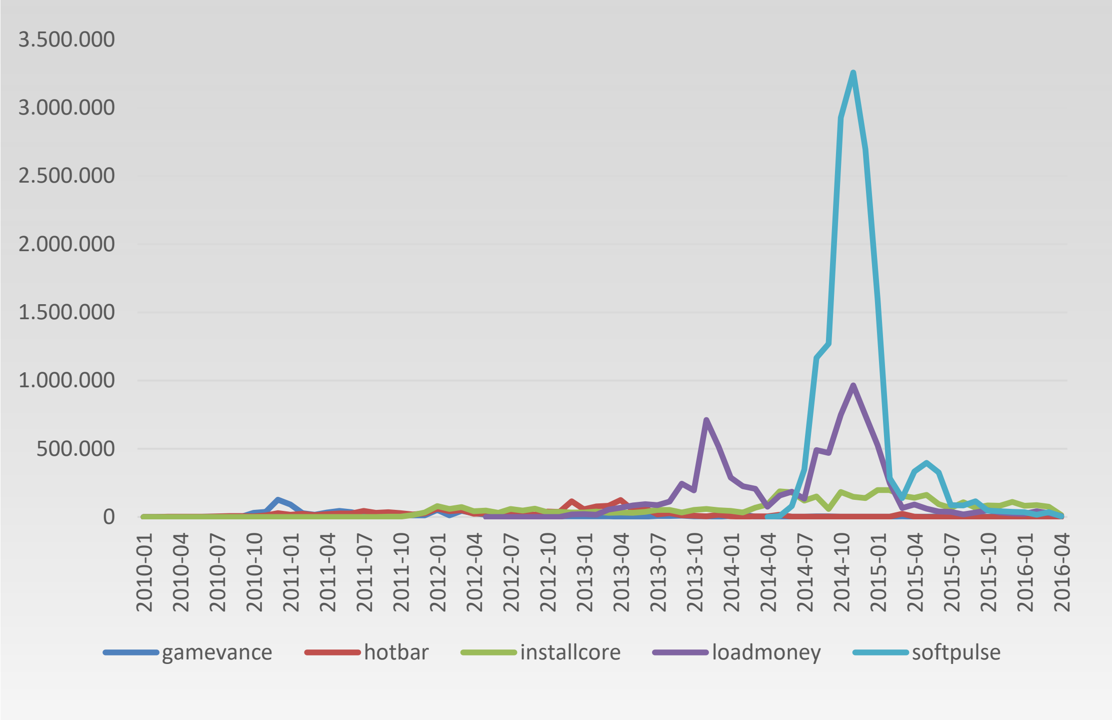
SOME STATISTICS FIRST

Prevalence and Distribution changed a lot during the years



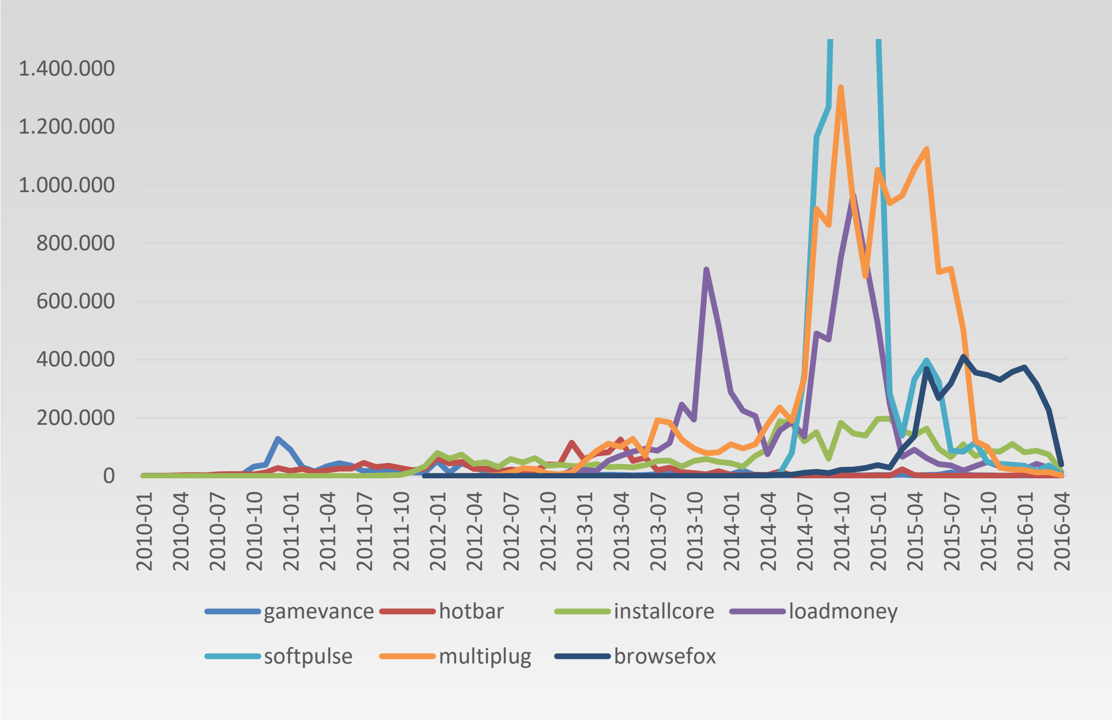
SOME STATISTICS FIRST

Prevalence and Distribution changed a lot during the years



SOME STATISTICS FIRST

Prevalence and Distribution changed a lot during the years



PUA, what is it ?

Wikipedia

“**Unwanted software bundling** is bundled software which computer users are fooled into installing along with a wanted program.”

- displays **intrusive advertising**
- **tracks the user's** Internet usage to sell information to advertisers
- **injects** its own **advertising** into web pages
- uses **premium SMS** services
- etc...

“The practice is widely considered *unethical* because it violates the *security interests* of users without their *informed consent*.”

SECURITY ISSUES ARISING

PUA and Security

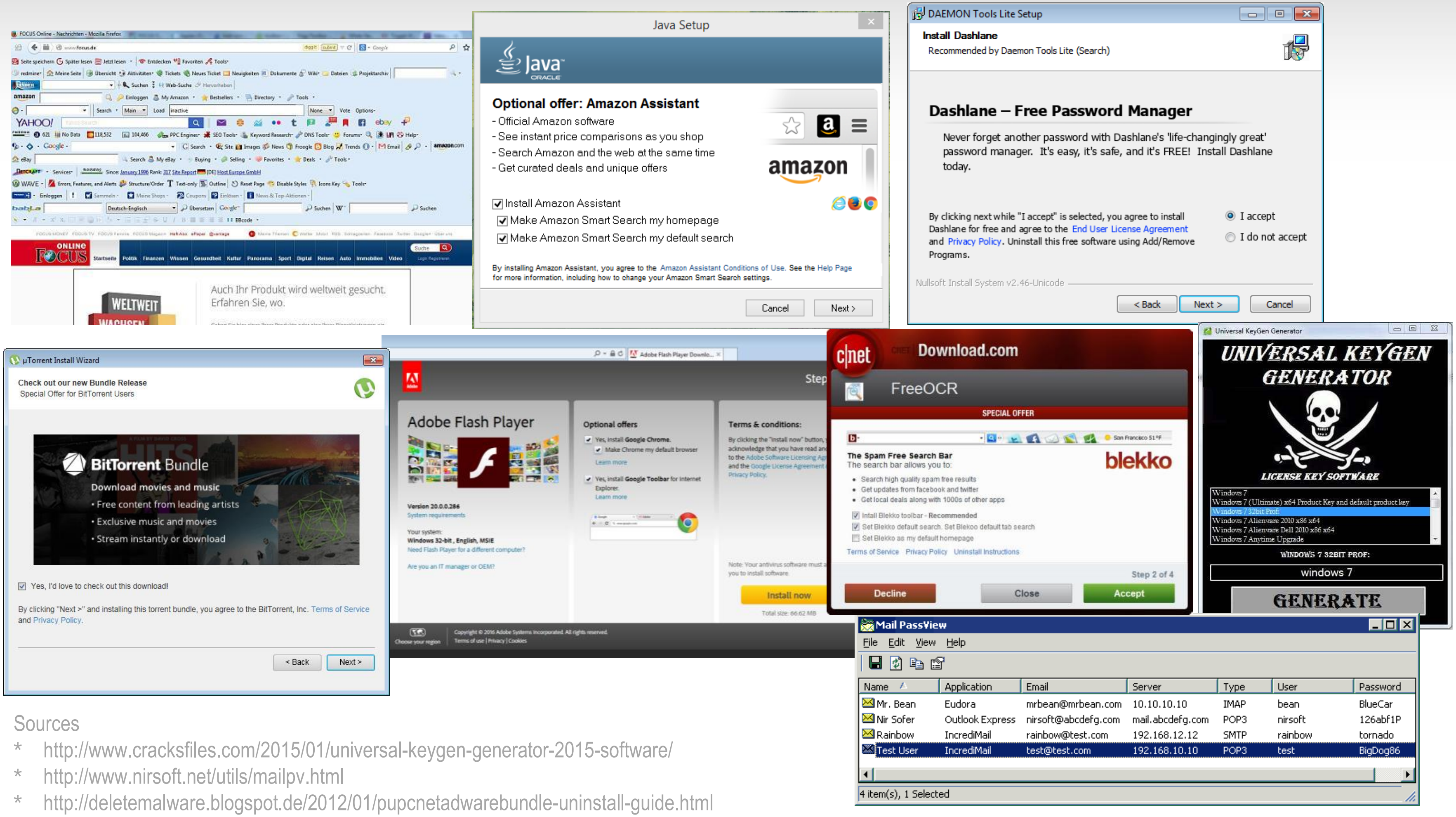
Wikipedia …

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

SOME PRETTY PICTURES



Auch Ihr Produkt wird weltweit gesucht. Erfahren Sie, wo.

Java Setup

Optional offer: Amazon Assistant

- Official Amazon software
- See instant price comparisons as you shop
- Search Amazon and the web at the same time
- Get curated deals and unique offers

☑ Install Amazon Assistant

☑ Make Amazon Smart Search my homepage

☑ Make Amazon Smart Search my default search

By installing Amazon Assistant, you agree to the Amazon Assistant Conditions of Use. See the Help Page for more information, including how to change your Amazon Smart Search settings.

DAEMON Tools Lite Setup

Install Dashlane

Recommended by Daemon Tools Lite (Search)

Dashlane – Free Password Manager

Never forget another password with Dashlane's 'life-changingly great' password manager. It's easy, it's safe, and it's FREE! Install Dashlane today.

By clicking next while "I accept" is selected, you agree to install Dashlane for free and agree to the End User License Agreement and Privacy Policy. Uninstall this free software using Add/Remove Programs.

● I accept

○ I do not accept

Nullsoft Install System v2.46-Unicode

µTorrent Install Wizard

Check out our new Bundle Release

Special Offer for BitTorrent Users

BitTorrent Bundle

Download movies and music

- Free content from leading artists
- Exclusive music and movies
- Stream instantly or download

☑ Yes, I'd love to check out this download!

By clicking "Next >" and installing this torrent bundle, you agree to the BitTorrent, Inc. Terms of Service and Privacy Policy.

Adobe Flash Player

Version 20.0.0.286

System requirements

Your system:

Windows 32-bit , English, MSIE

Need Flash Player for a different computer?

Are you an IT manager or OEM?

Optional offers

☑ Yes, install **Google Chrome.**

☑ Make Chrome my default browser

Learn more

☑ Yes, install **Google Toolbar** for Internet Explorer.

Learn more

Terms & conditions:

By clicking the "Install now" button, y acknowledge that you have read an to the Adobe Software Licensing Ag and the Google License Agreement Privacy Policy.

Note: Your antivirus software must a you to install software

Total size: 66.62 MB

Copyright © 2016 Adobe Systems Incorporated. All rights reserved.

FreeOCR

SPECIAL OFFER

The Spam Free Search Bar

The search bar allows you to:

- Search high quality spam free results
- Get updates from facebook and twitter
- Get local deals along with 1000s of other apps

☑ Intall Blekko toolbar - **Recommended**

☑ Set Blekko default search. Set Blekoo default tab search

□ Set Blekko as my default homepage

Terms of Service Privacy Policy Uninstall Instructions

Step 2 of 4

Universal KeyGen Generator

UNIVERSAL KEYGEN GENERATOR

LICENSE KEY SOFTWARE

```
Windows 7
Windows 7 (Ultimate) x64 Product Key and default product key
Windows 7 32bit Prof:
Windows 7 Alienware 2010 x86 x64
Windows 7 Alienware Dell 2010 x86 x64
Windows 7 Anytime Upgrade
```

WINDOWS 7 32BIT PROF:

windows 7

Mail PassView

Name	Application	Email	Server	Type	User	Password
Mr. Bean	Eudora	mrbean@mrbean.com	10.10.10.10	IMAP	bean	BlueCar
Nir Sofer	Outlook Express	nirsoft@abcdefg.com	mail.abcdefg.com	POP3	nirsoft	126abf1P
Rainbow	IncrediMail	rainbow@test.com	192.168.12.12	SMTP	rainbow	tornado
Test User	IncrediMail	test@test.com	192.168.10.10	POP3	test	BigDog86

4 item(s), 1 Selected

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

EVERYBODY’S GOT TO EAT

Monetarization

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

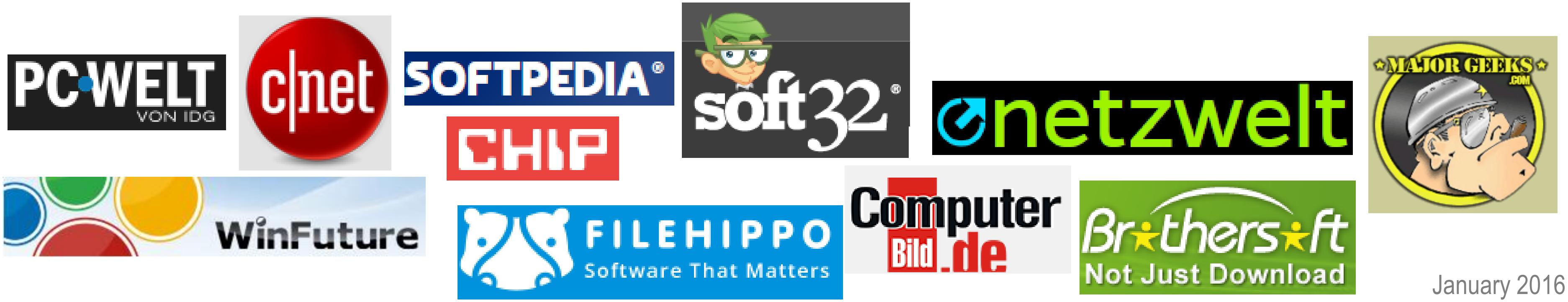
- Distribution through bundlers
- Information Harvesting
- Aggressive Advertisement

TEST SETUP

Experiment Setup

Snapshot from one point in time (January 2016)

- Looking at **11 of the top 15 Download portals** (according to Alexa)
- Creating ranking of most distributed applications over all portals
- Downloading (and comparing) **21 most popular applications**
- Analysing with AV-TEST in-house tools
- ….

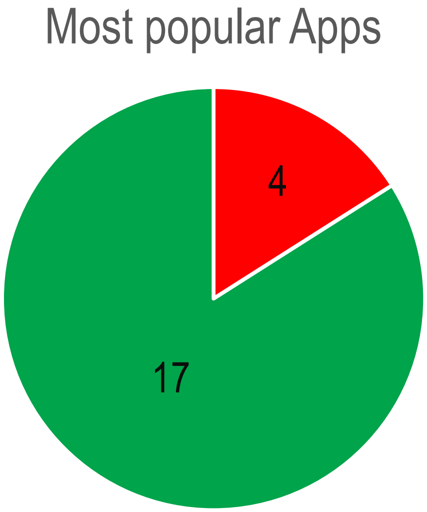


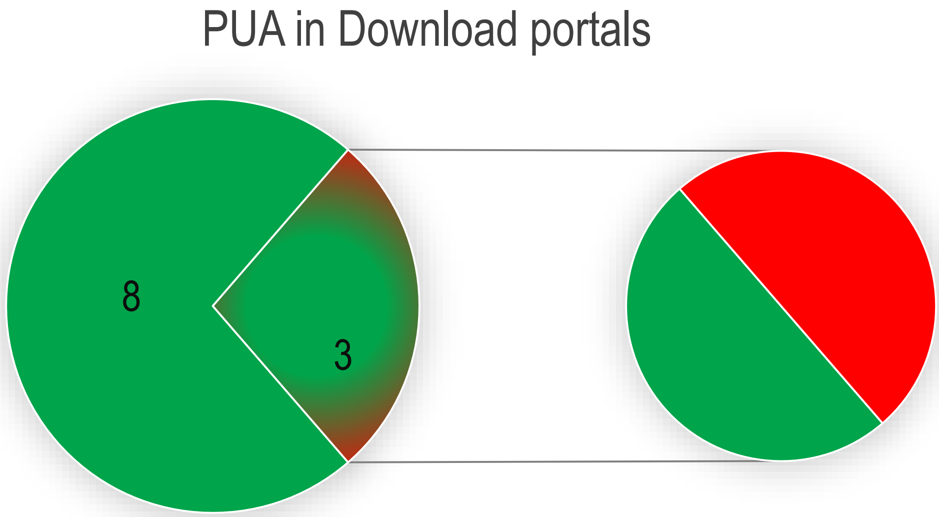
January 2016

PUA found on Portals

PUA

Clean





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

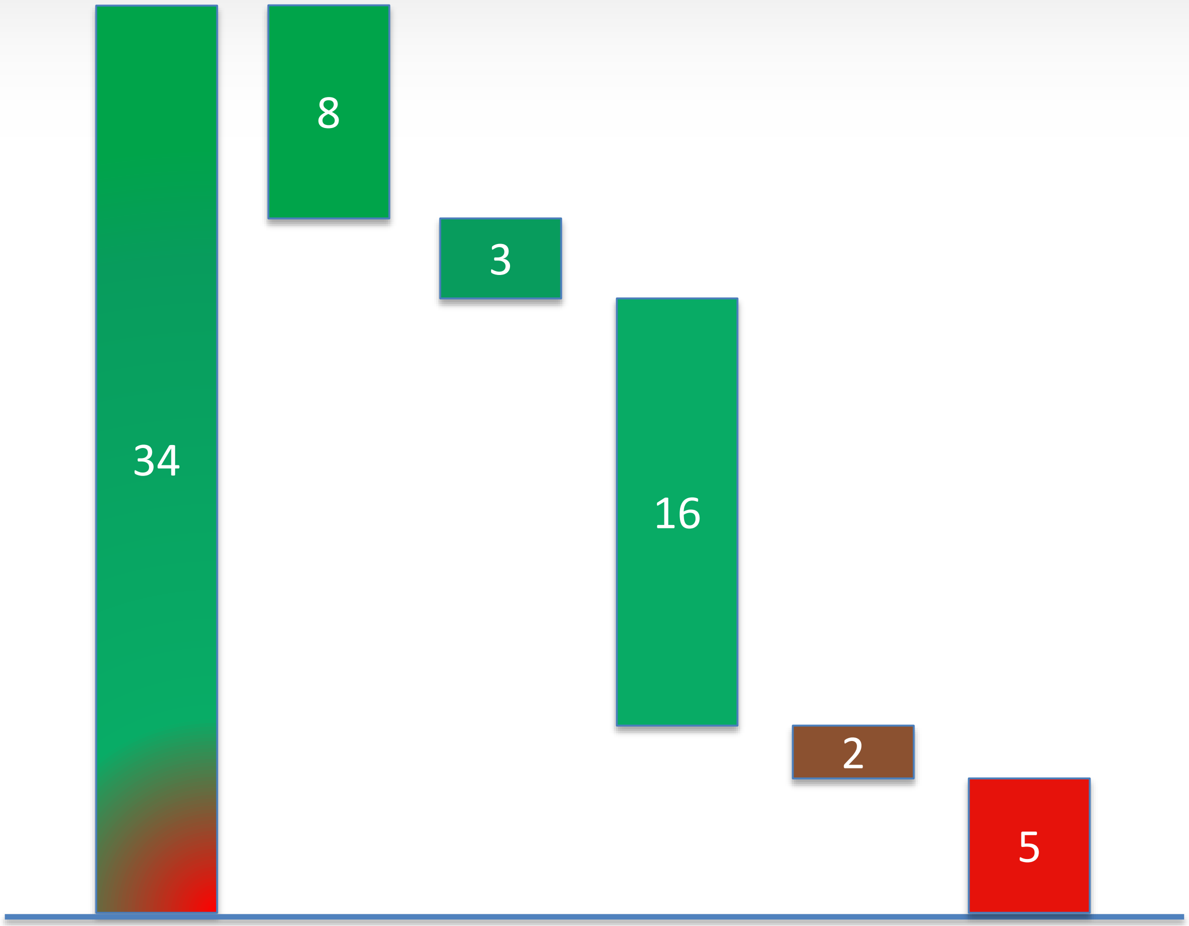
…

And provide protection against disruptive software

PUA DETECTION BY DEFAULT?

AV

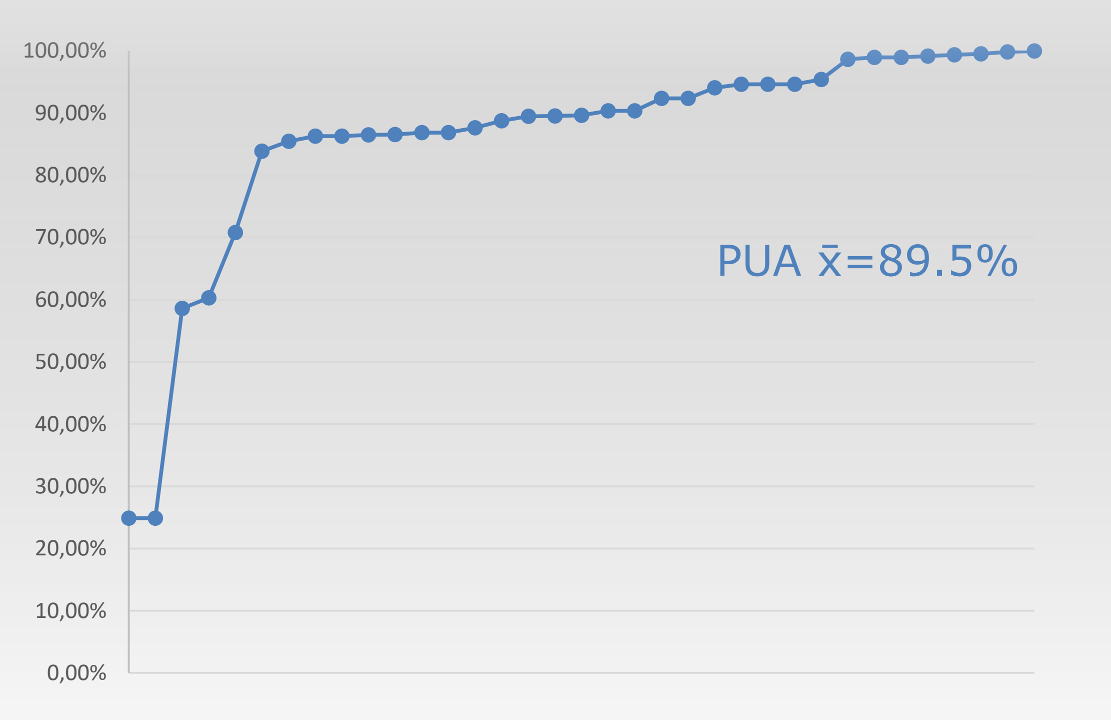
Default Settings



January 2016

PUA DETECTION (WINDOWS)

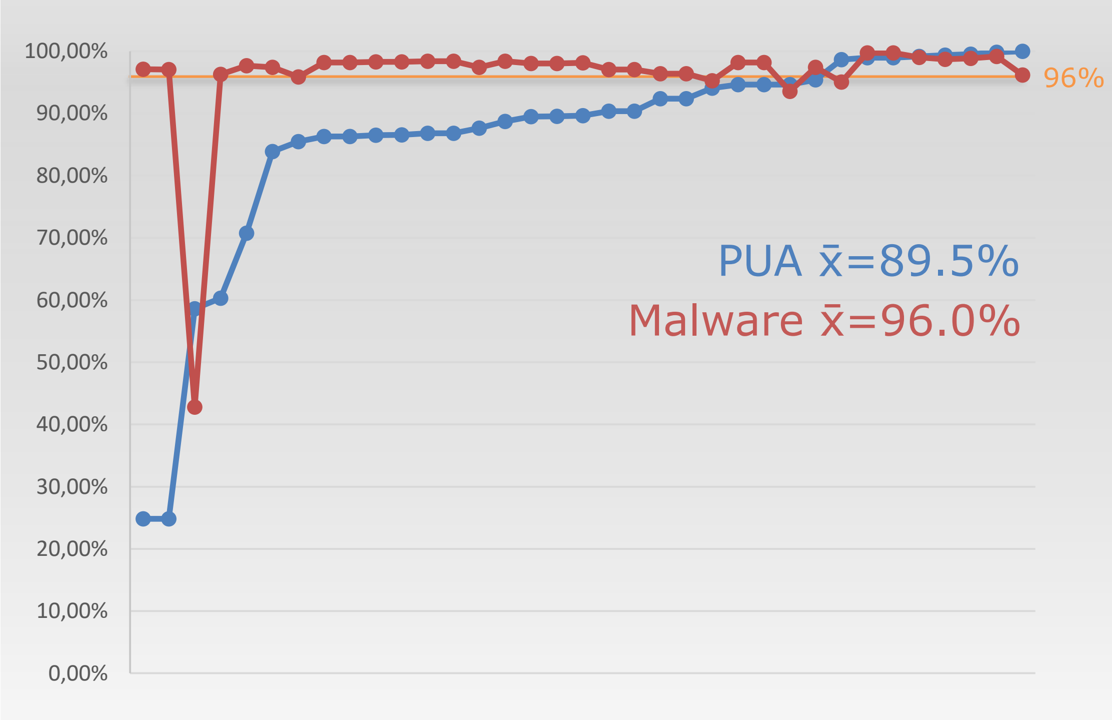
PUA detection
Rate per product
(on-demand)



January 2016

PUA VS MALWARE DETECTION (WINDOWS)

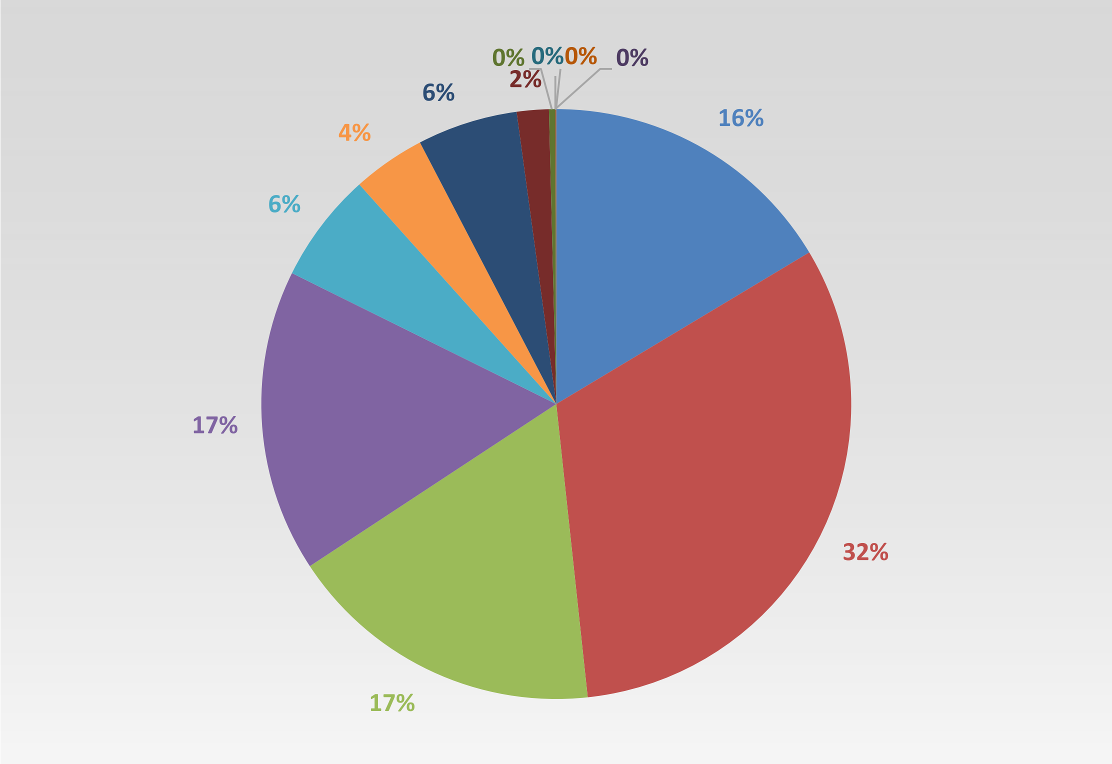
PUA detection Rate vs. Malware detection per product (on-demand)



January 2016

DIGITALLY SIGNED PUA FILES

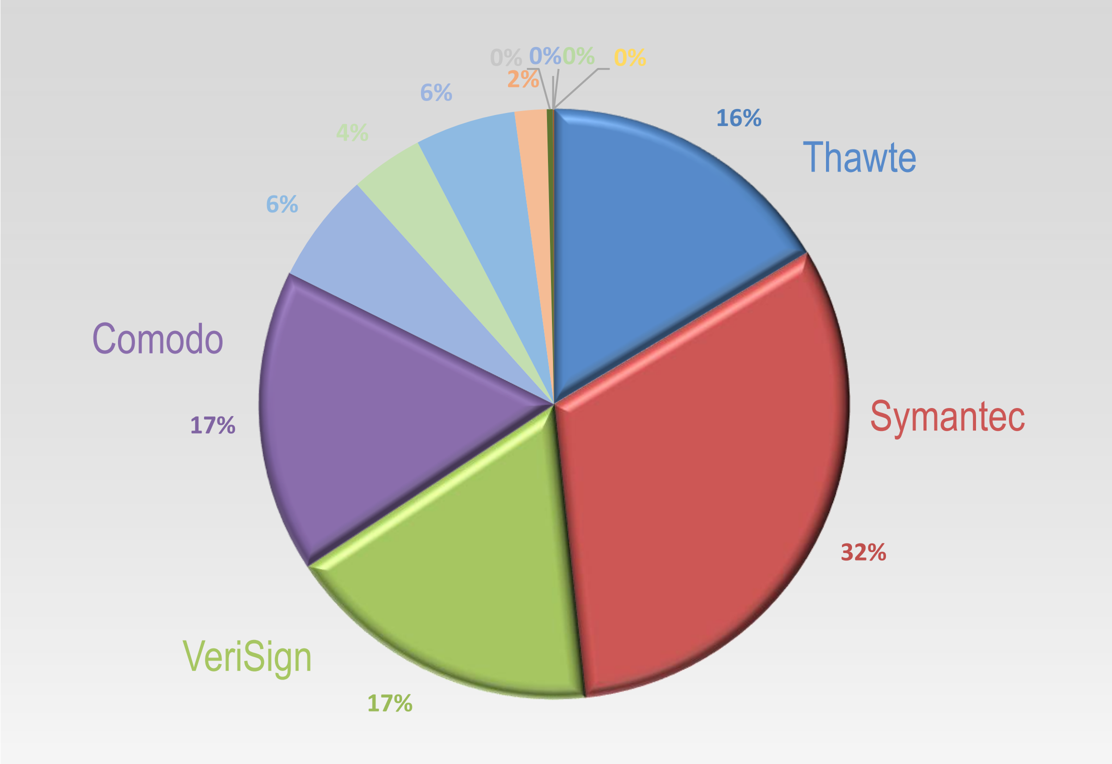
PUA files signed by different certificate authorities



July 2015

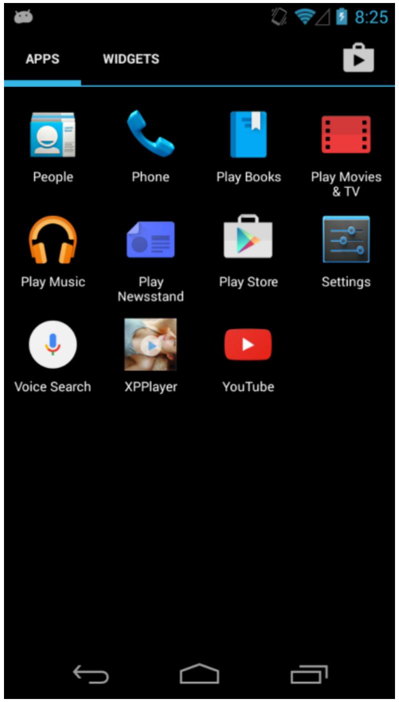
DIGITALLY SIGNED PUA FILES CONFLICT OF INTEREST ?

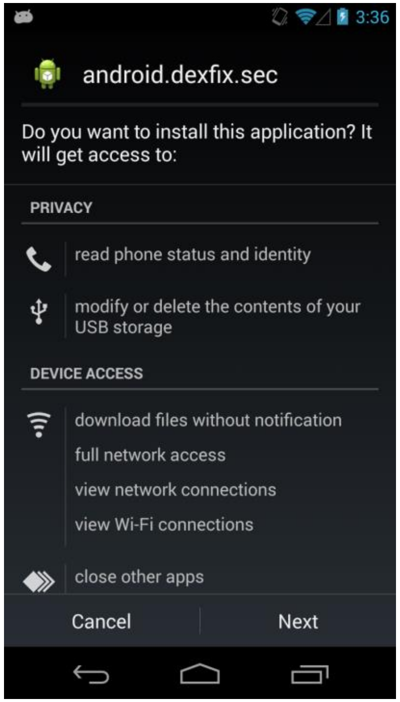
PUA files signed by different AV industry related certificate authorities



July 2015

NOT JUST WINDOWS IS AFFECTED … ALSO ANDROID





android.dexfix.sec

Do you want to install this application? It will get access to:

PRIVACY

read phone status and identity

modify or delete the contents of your USB storage

DEVICE ACCESS

download files without notification

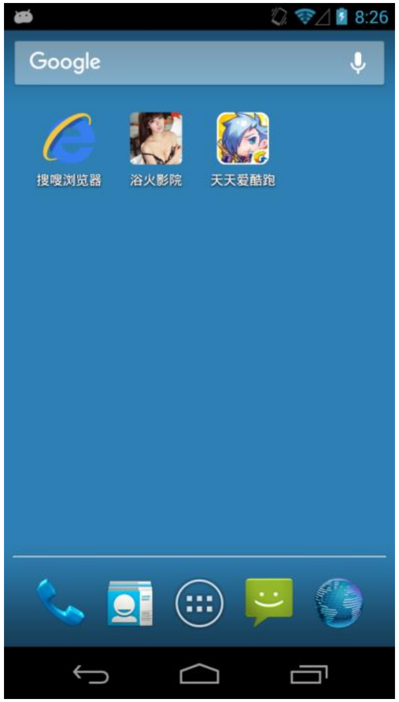
full network access

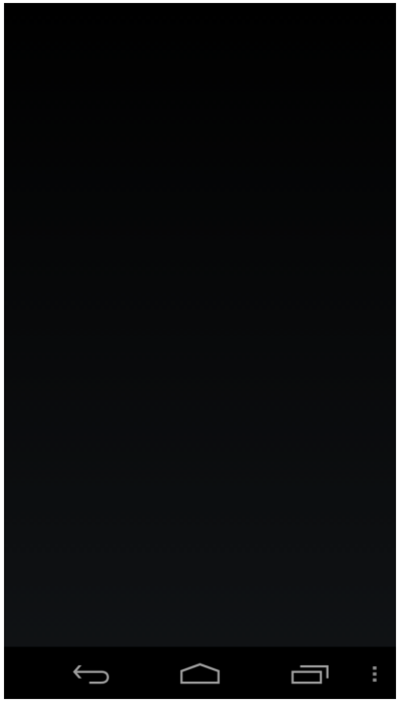
view network connections

view Wi-Fi connections

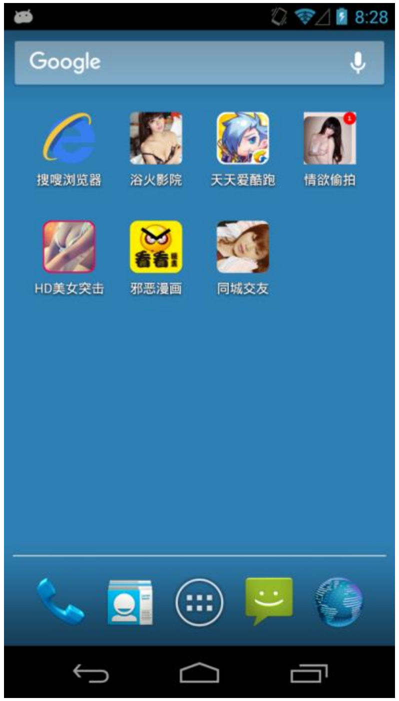
close other apps

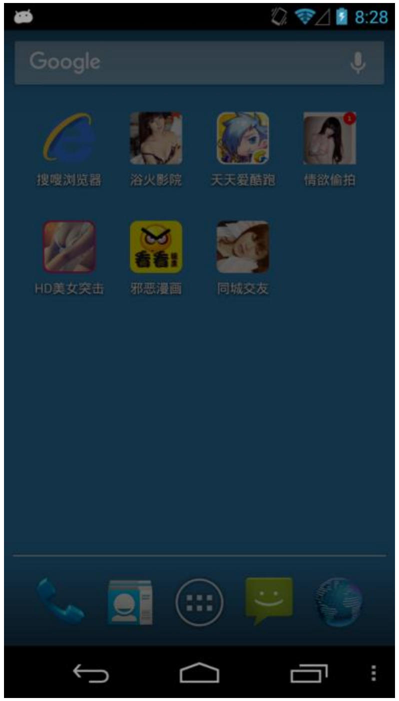
Cancel | Next

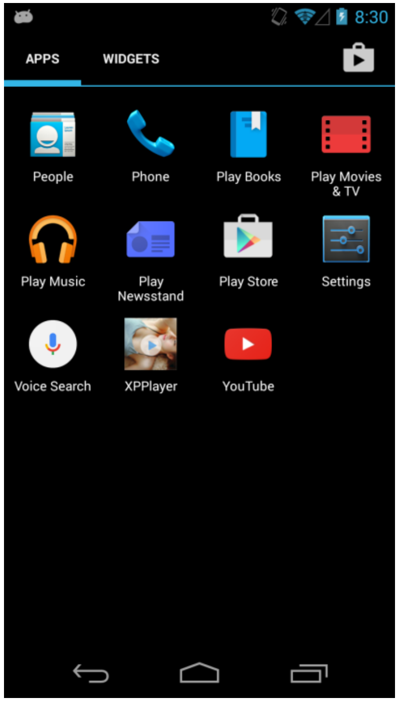


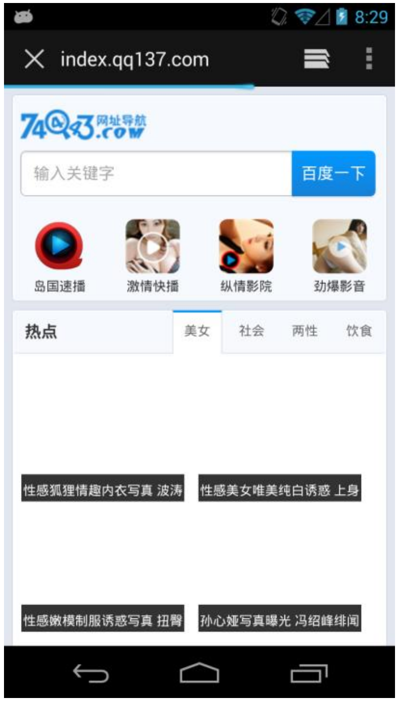


NOT JUST WINDOWS IS AFFECTED …



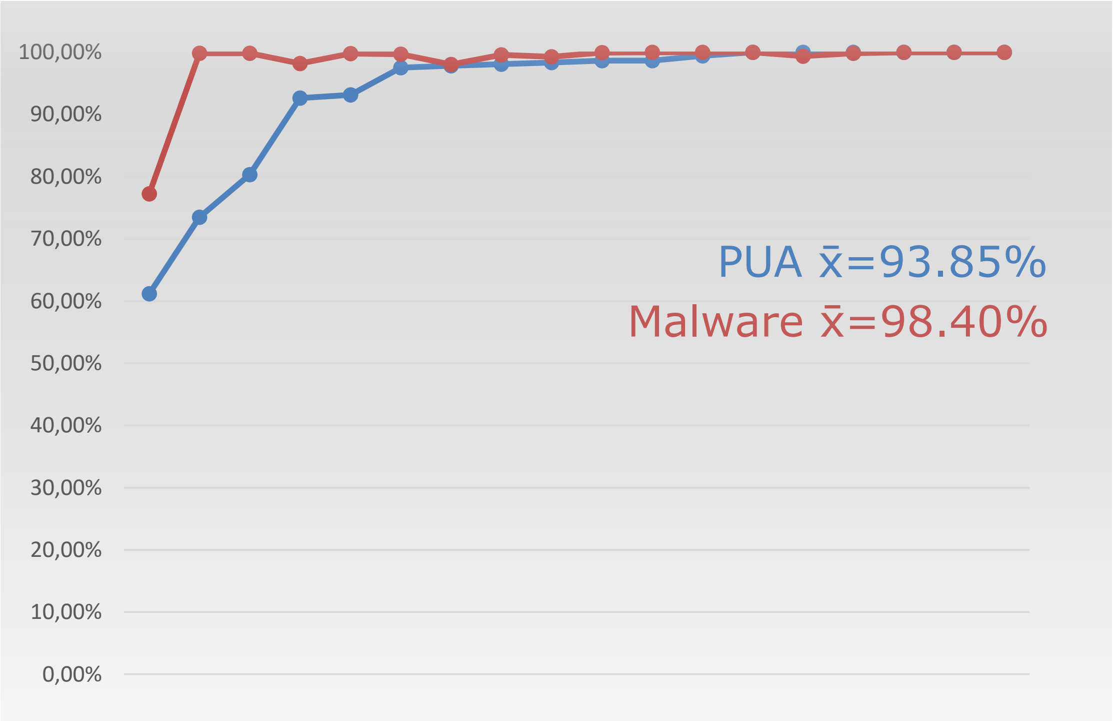






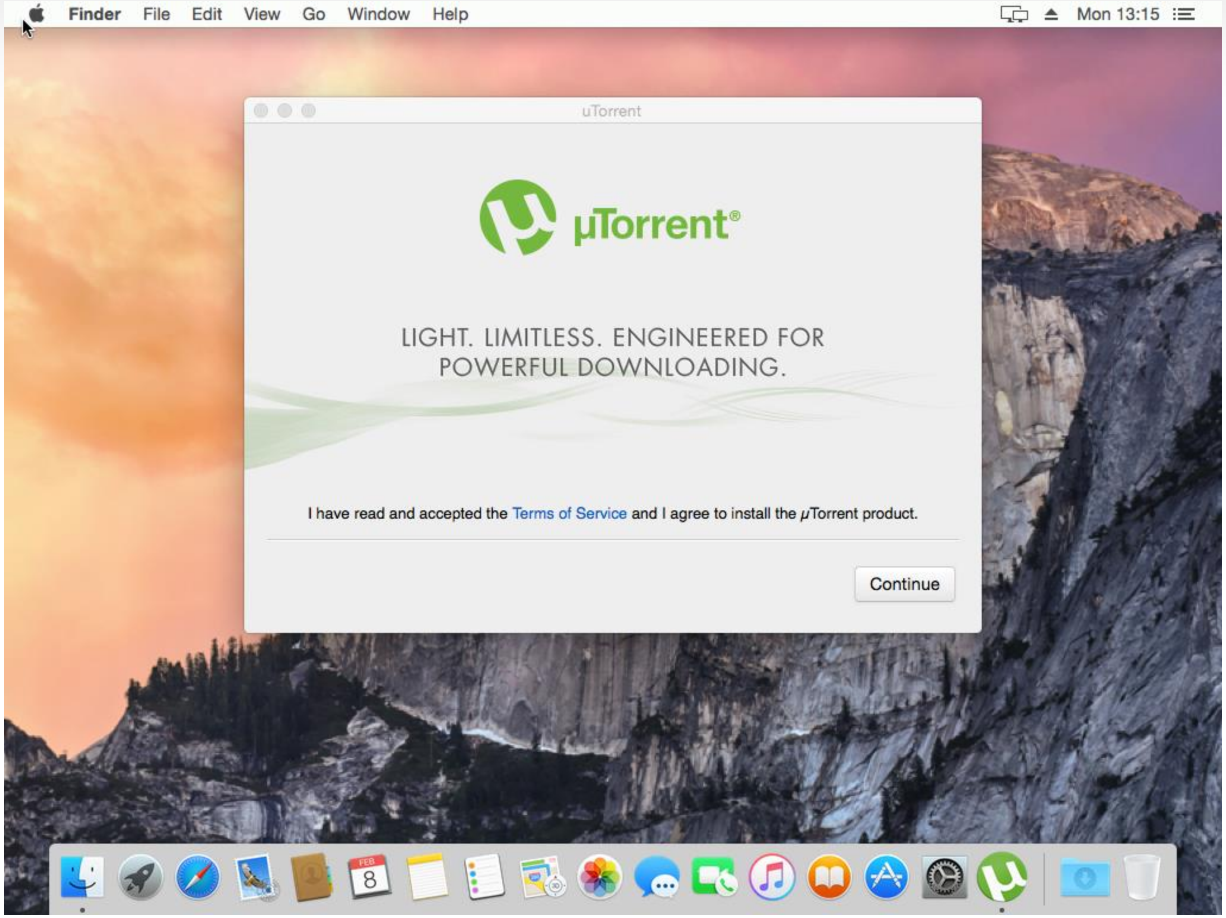
PUA DETECTION VS MALWARE DETECTION (ANDROID)

PUA detection Rate vs. Malware detection per product



January 2016

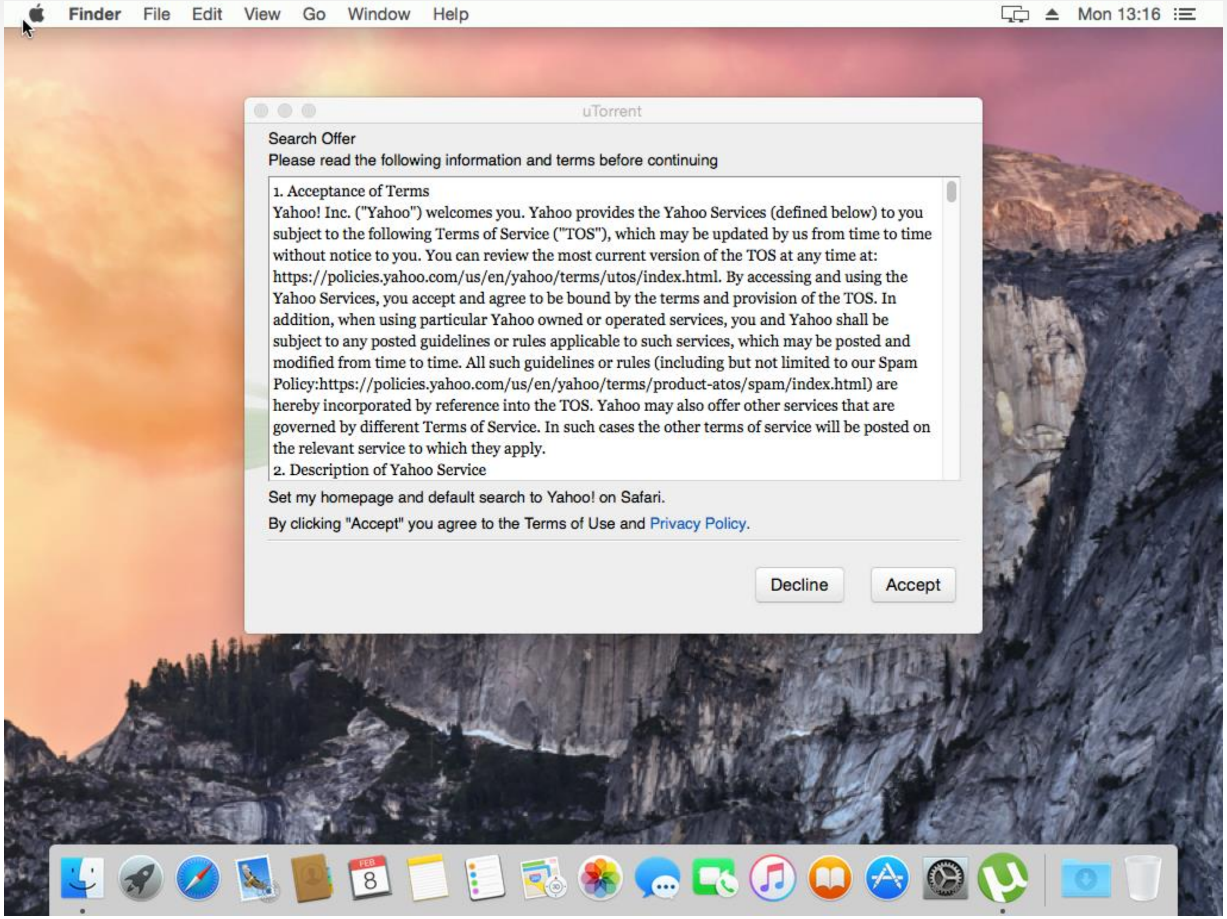
… ALSO MAC OS



LIGHT. LIMITLESS. ENGINEERED FOR POWERFUL DOWNLOADING.

I have read and accepted the Terms of Service and I agree to install the µTorrent product.

...



Search Offer

Please read the following information and terms before continuing

1. Acceptance of Terms

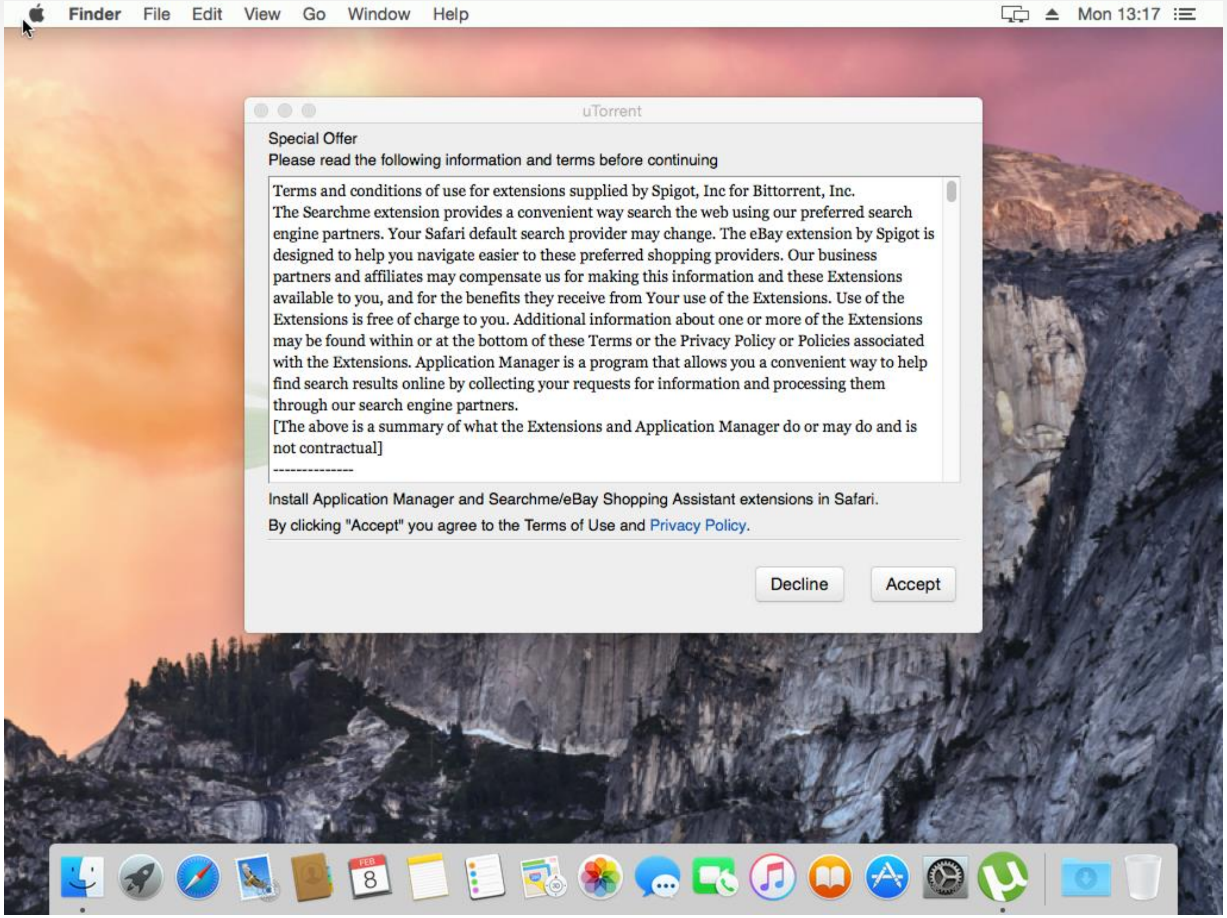
Yahoo! Inc. ("Yahoo") welcomes you. Yahoo provides the Yahoo Services (defined below) to you subject to the following Terms of Service ("TOS"), which may be updated by us from time to time without notice to you. You can review the most current version of the TOS at any time at: https://policies.yahoo.com/us/en/yahoo/terms/utos/index.html. By accessing and using the Yahoo Services, you accept and agree to be bound by the terms and provision of the TOS. In addition, when using particular Yahoo owned or operated services, you and Yahoo shall be subject to any posted guidelines or rules applicable to such services, which may be posted and modified from time to time. All such guidelines or rules (including but not limited to our Spam Policy:https://policies.yahoo.com/us/en/yahoo/terms/product-atos/spam/index.html) are hereby incorporated by reference into the TOS. Yahoo may also offer other services that are governed by different Terms of Service. In such cases the other terms of service will be posted on the relevant service to which they apply.

2. Description of Yahoo Service

Set my homepage and default search to Yahoo! on Safari.

By clicking "Accept" you agree to the Terms of Use and Privacy Policy.

...



Special Offer

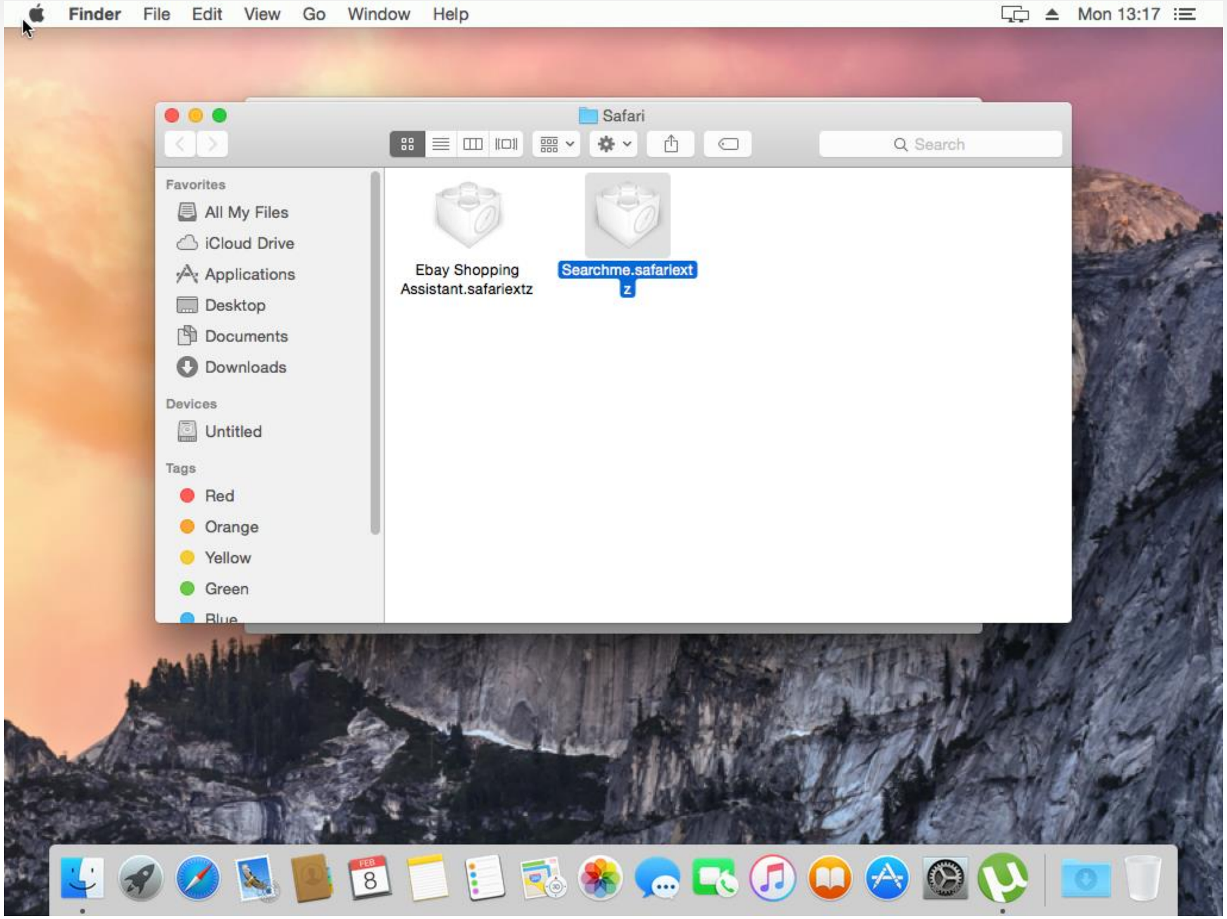
Please read the following information and terms before continuing

Terms and conditions of use for extensions supplied by Spigot, Inc for Bittorrent, Inc.
The Searchme extension provides a convenient way search the web using our preferred search engine partners. Your Safari default search provider may change. The eBay extension by Spigot is designed to help you navigate easier to these preferred shopping providers. Our business partners and affiliates may compensate us for making this information and these Extensions available to you, and for the benefits they receive from Your use of the Extensions. Use of the Extensions is free of charge to you. Additional information about one or more of the Extensions may be found within or at the bottom of these Terms or the Privacy Policy or Policies associated with the Extensions. Application Manager is a program that allows you a convenient way to help find search results online by collecting your requests for information and processing them through our search engine partners.
[The above is a summary of what the Extensions and Application Manager do or may do and is not contractual]

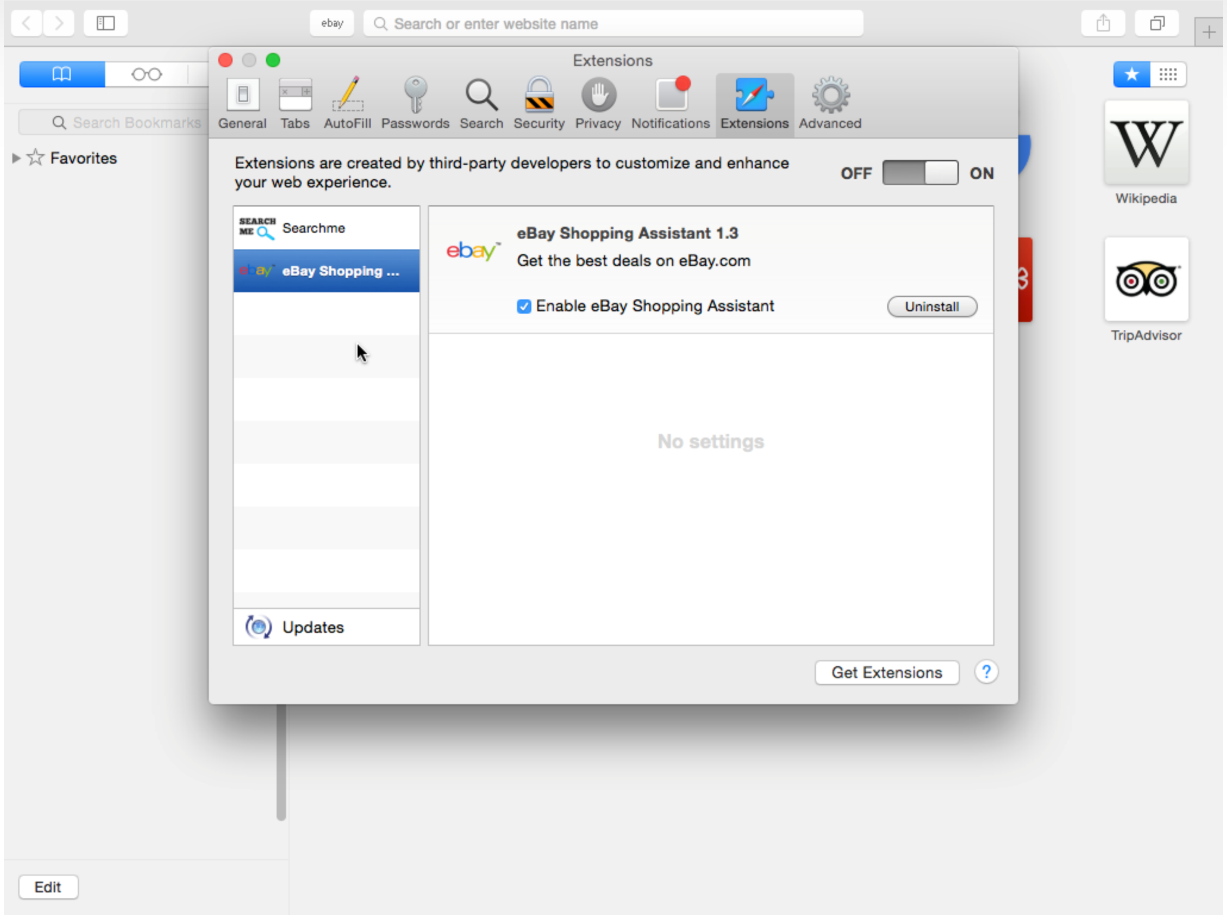
Install Application Manager and Searchme/eBay Shopping Assistant extensions in Safari.

By clicking "Accept" you agree to the Terms of Use and Privacy Policy.

...


Finder File Edit View Go Window Help
Mon 13:17
Safari
Search
Favorites
All My Files
iCloud Drive
Applications
Desktop
Documents
Downloads
Devices
Untitled
Tags
Red
Orange
Yellow
Green
Blue
Ebay Shopping Assistant.safariextz
Searchme.safariextz

...



Extensions are created by third-party developers to customize and enhance your web experience.

OFF ● ON

eBay Shopping Assistant 1.3

Get the best deals on eBay.com

☑ Enable eBay Shopping Assistant

CONCLUSION

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

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

Users expect AV to protect or at least warn them.

Big **differences between vendors** on how to approach PUA.

Industry wide **rules are missing**.

Is **CSA helping or is it causing more trouble?** Is it driven by the right parties and with the right motivation?

@avtestorg (English) & @avtestde (German)

Follow us on facebook.com/avtestorg

Current test results at https://www.av-test.org

Thank you for your attention!