PUA: Distribution and Detection
ABOUT AV-TEST

The AV-TEST Institute in Magdeburg
New scary numbers every year!

More Malware than ever before!

Just Malware?
Development of Malware and PUA for Windows from 2010 to now

266 Million files received with at least 5 detections
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 66 Million files
SOME STATISTICS FIRST

Prevalent PUA Families per year

Families have their ups and downs

Number of prevalent families increased
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
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
Sources
* http://www.nirsoft.net/utils/mailpv.html
* http://deletemalware.blogspot.de/2012/01/pupcnetadwarebundle-uninstall-guide.html
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
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
- ....

[Images of various download portals and software logos]
PUA found on Portals

Most popular Apps

PUA: 4
Clean: 17

PUA in Download portals

8 total
3 PUA
5 Clean
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
Rate per product
(on-demand)

PUA $\bar{x} = 89.5\%$
PUA vs. Malware Detection (Windows)

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

PUA $\bar{x} = 89.5\%$

Malware $\bar{x} = 96.0\%$

January 2016
PUA files signed by different certificate authorities
PUA files signed by different AV industry related certificate authorities

July 2015
NOT JUST WINDOWS IS AFFECTED … ALSO ANDROID
NOT JUST WINDOWS IS AFFECTED …
PUA detection Rate vs. Malware detection per product

PUA $\bar{x} = 93.85\%$

Malware $\bar{x} = 98.40\%$

January 2016
... ALSO MAC OS

![Image of Mac OS with uTorrent installation window]

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

Continue
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/sas/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-sas/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.

Decline  Accept
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 Searchmax extension provides a convenient way to 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 Searchmax/eBay Shopping Assistant extensions in Safari.
By clicking "Accept" you agree to the Terms of Use and Privacy Policy.

Decline  Accept
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!