

Industry approach for **Unwanted Software Criteria & Clean Requirements**

Jiří Sejtko, AVAST

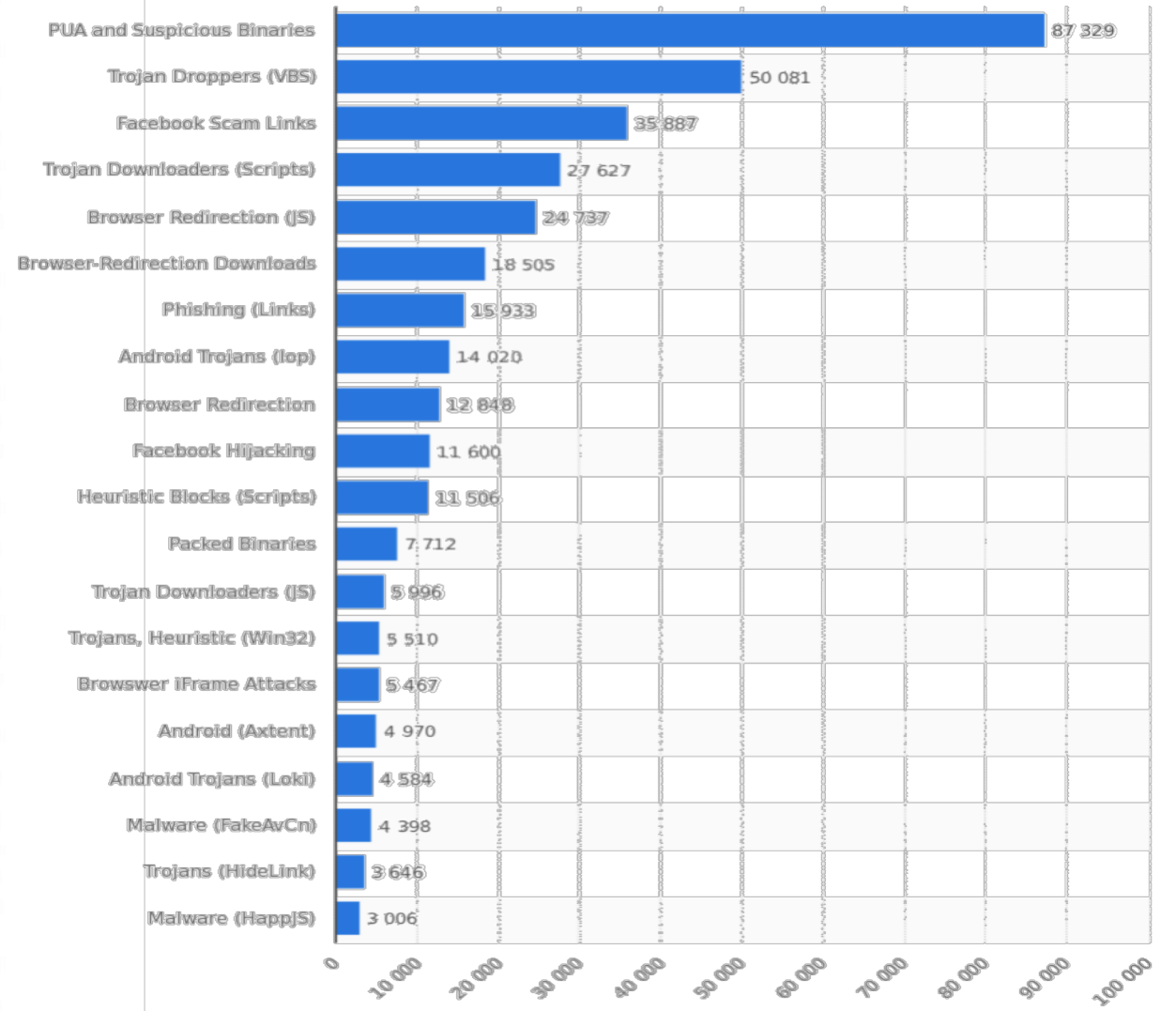
Alexander Vukcevic, Avira

2018-10



Industry approach for Unwanted Software Criteria & Clean Requirements

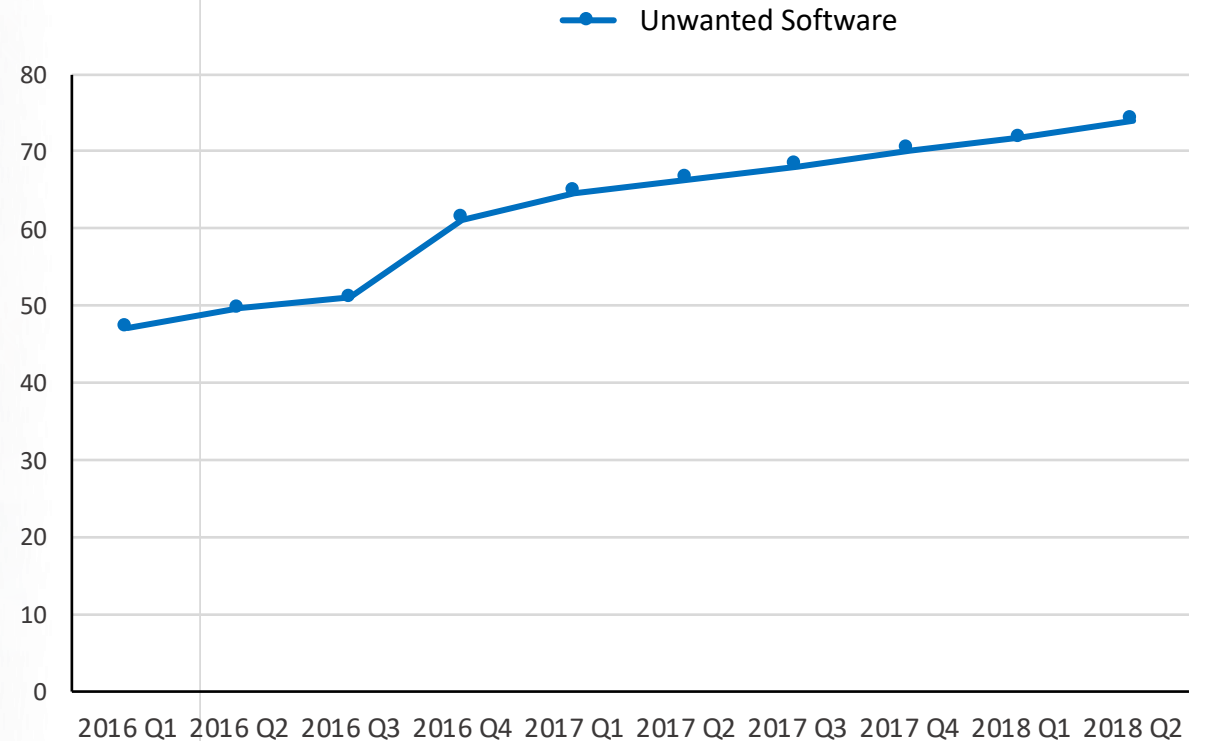
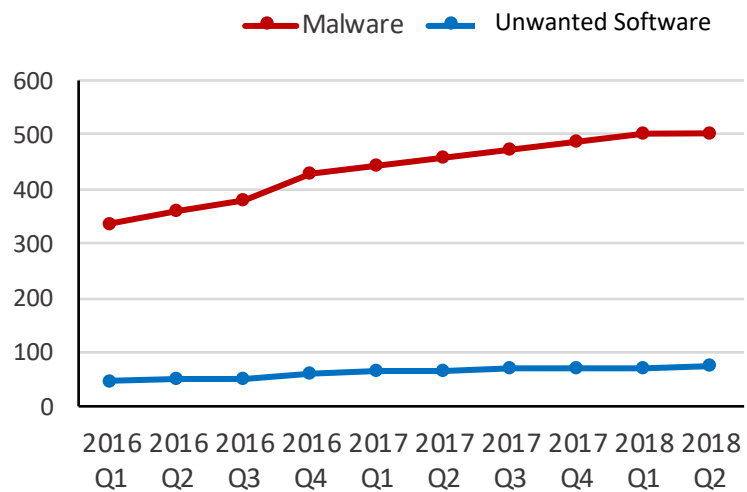
Most commonly observed types of malware worldwide in 2016, by detected sample count



Source: Worldwide; Cisco Systems; Statista 2018

Industry approach for Unwanted Software Criteria & Clean Requirements

Motivation



In millions. Source: Avira Protection Services, 2018

Industry approach for Unwanted Software Criteria & Clean Requirements

Motivation

Standing today..

- .. there is no common agreement in the security industry for USC
- .. not all antivirus companies are sharing their guidelines in public
- .. no public space for common industry USC guidelines
- .. AppEsteem & CSA guidelines have no official industry approval
- .. there is no possibility to review all guidelines on a single space

- .. and there is no transparency about how good your AV is protecting you against potential unwanted application and software components

Industry approach for Unwanted Software Criteria & Clean Requirements

Motivation

AppEsteem has done a good job highlighting the need for unified series of requirements applied to the Unwanted Software space.

But we are missing attribution.

The industry would be better served if an independent organization maintained the collective set of rules and policies enforced by security companies. The desire is that this repository will lead to a common alignment of what is and is not acceptable while preserving each security company right to follow their own criteria.

This criteria can be used by CSA, AppEsteem and others in certification of apps which not violate these rules.

Industry approach for Unwanted Software Criteria & Clean Requirements

The value proposition

1. A one stop shop for monetization companies to see what the rules are, and what the effect of violating the rules would be
2. A one stop shop for certification companies to see what they need to be measuring
3. A place for testers to learn what behaviour to expect from security software
4. A place for security vendors to disclose their policies
5. Rule documentation includes list of software, screenshots with corrections, metadata, documentation, sample exchange

Industry approach for Unwanted Software Criteria & Clean Requirements

The value proposition

An independent organisation body must be formed..

This organisation wont certify clean nor flag PUAs apps, **it just holds a list of unwanted software criteria (USC)**, document and align on them. This USC repository will be freely accessible to everyone – and can be used as industry guidance for CSA, CleanApps, or any software distributor to avoid flagging by the anti-malware industry.

The group is independent and USC requirement list is managed by the AV industry.

Feedback and recommendations from other organisation like CSA, CleanApps or others are welcomed. New USC requirements being discussed and can be followed by each of the members independently.

Industry approach for Unwanted Software Criteria & Clean Requirements

AMTSO as umbrella association?

- Establishing a new organisation is time consuming, and must be set to operational (executive board, advisory board, etc.)
- Members have to pay an additional fee for membership.
- Security companies, testers and a certifier are already members of AMTSO (<https://www.amtso.org/members/>)
- AMTSO has proved that it can solve multi-stakeholder problems.



AMTSO is well suited and positioned to be the body that maintains this list of policies, known as Unwanted Software Criteria (USC). As an independent body AMTSO can facilitate the creation of additional certification bodies and serve those already in existence.

Industry approach for Unwanted Software Criteria & Clean Requirements

AMTSO as umbrella association?

Criteria Working Group under AMTSO



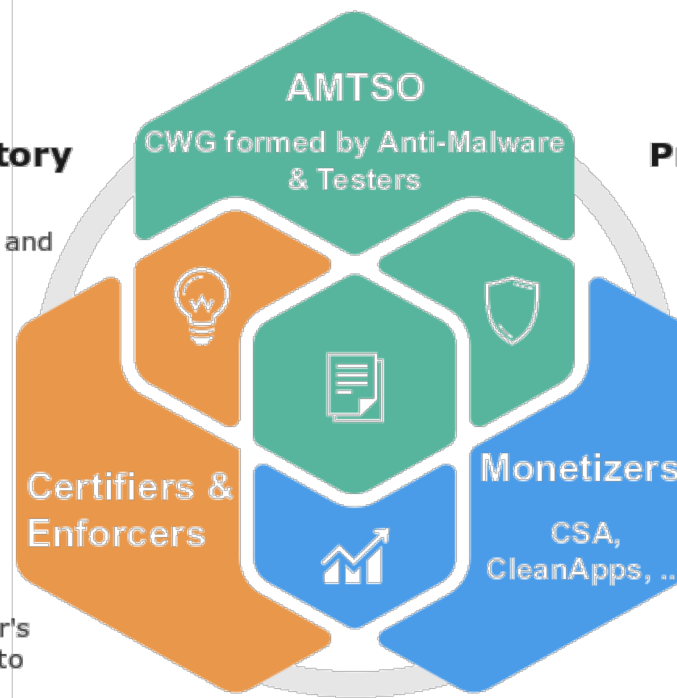
Criteria Repository

CWG is collecting, documenting, aligning and attributing submitted criteria to keep Anti-Malware industry on track.



Transparency

Certifiers follow vendor's criteria or let vendors to adopt their own. Certification or blacklisting is transparent. In addition, detections can be outsources to these bodies.



Protection & Testing

Anti-Malware vendors alignment on their criteria and latest practices keeps their users safe. Testers are able to select and measure the vendors's effectiveness against Unwanted Software



One stop shop

One place to understand what is not acceptable, to communicate with industry as well as the place for suggestions to published criteria.

Industry approach for Unwanted Software Criteria & Clean Requirements

Thanks

Any questions?

Jiří Sejtko, AVAST
Alexander Vukcevic, Avira
Mark Kennedy, Symantec



Draft: Industry approach for Unwanted Software Criteria & Clean Requirements: <http://bit.ly/USCApproach>