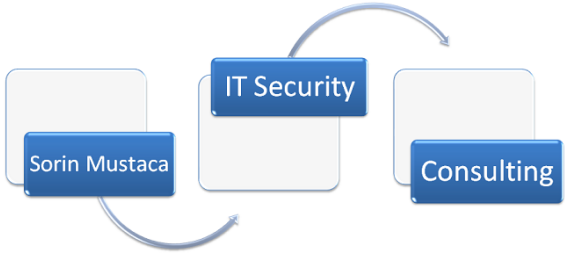


CHALLENGES FOR YOUNG ANTI-MALWARE PRODUCTS TODAY

SORIN MUSTACA

CEO, SORIN MUSTACA IT SECURITY CONSULTING UG(Hfb)

ABOUT ME

- Started to work in security at RAV Antivirus (~20 years ago)
- Worked at Avira (11y) in various roles (Eng., PM), at Honeywell as product security leader
- In 2015 founded my own company – www.mustaca.com
- I help companies to integrate technologies and build AM products
- BTW: I also wrote a book about security, by I will not give it here – it is free ;)
- I have been attending this conference for quite a lot of times

(but not as often as others here ☺)

CHALLENGES FOR YOUNG ANTI-MALWARE PRODUCTS TODAY

- Target audiences:
  - new commers in the AM industry, companies building AM solutions for endpoints
    - For them I will offer during the presentation **Advices** (free) ;)
  - Rest of you, reminder how hard it is
- Many of you work for an established AM company, having mature security products & technologies

Challenges:

- Be impartial
- Make this presentation interesting for everybody

GOALS

- **High level tasks/Contents:**

  Build a “simple” antimalware product for Windows 7, 8.x, 10+ :

  1. The Scanner: On Demand and On Access scanning
  2. Collect GDPR-conform Telemetry data
  3. Testing and certifications
  4. Integration with Windows Security Center
  5. Go to market strategy
     - How to keep a good reputation
     - How not to be flagged by the industry
     - Free product?

HOLD ON!!!

Is that all what an AM product has?

NO!

There are many other items needed to build even the simplest AM product, but we must ignore them in this presentation due to time constraints (30 min)

Feel free to ask me more in the break.

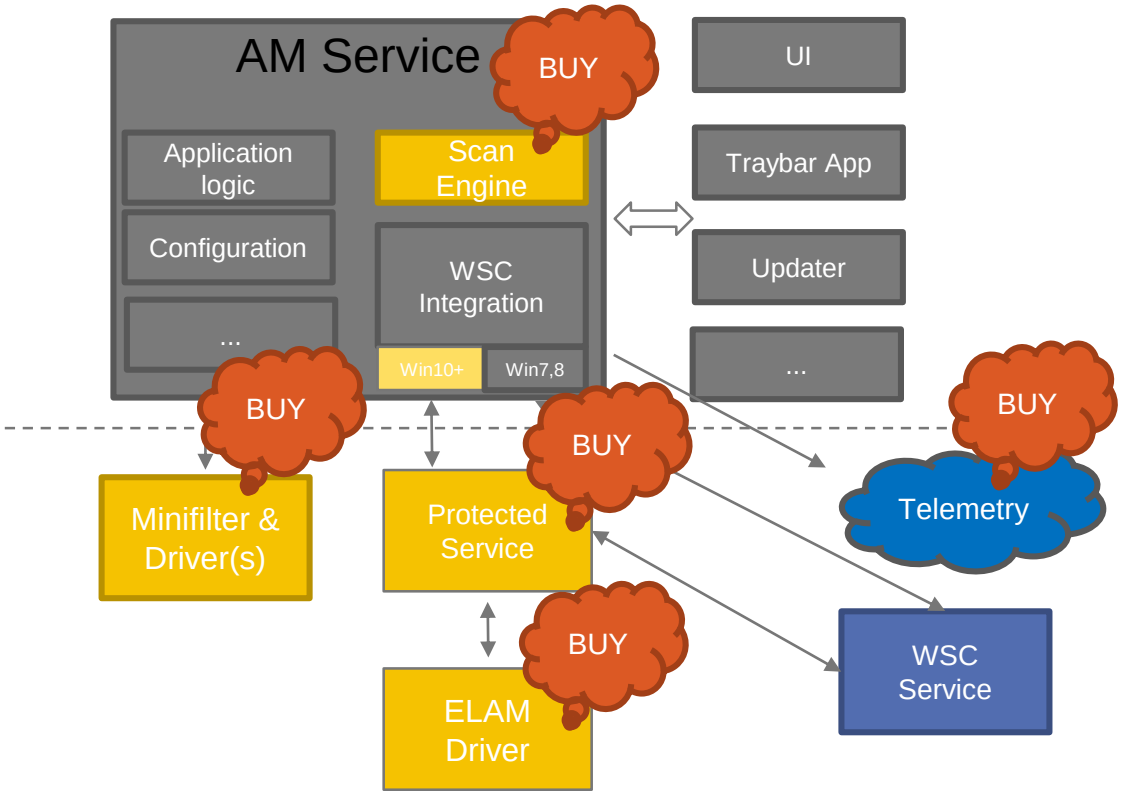
1.THE SCANNER

- **OEM detection engine, ideally with optional cloud based zero-day detection:**
  - all are very good
  - have stable APIs available in various languages (C/C++, C#)
  - differ in pricing and conditions:
- On Access scanning functionality: file access interception through minifilter and/or drivers

Advices:

- small companies should ask for “startup” conditions
- ask also about WSC integration (more later)

THE BIG (SIMPLIFIED) PICTURE



Build vs. Buy

Build:

AM Service, UI, Traybar App, Updater,etc.

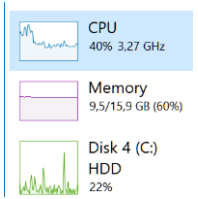
Buy(License):

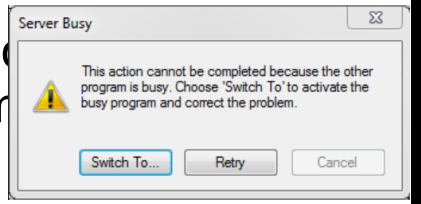
Scan engine, Minifilter, PS, ELAM Drv., Connection to a Telemetry/Statistics cloud service

1. THE SCANNER – NON-FUNCTIONAL FEATURES

The product should be:

- **Reliable**: it doesn't crash, it does what it says it does, it is prepared to detect also "tricky malware"
- **Resilient**: is not (easily) hackable, it can't be killed, it restarts if it was killed
- **Performant**: it doesn't slow down the computer too much (<10%), it doesn't impact the usability of other programs
- **Testable**: create special logs with the detections, doesn't c and doesn't overload the computer when a few hundred m samples are scanned
- **Certifiable**: not important at the beginning, but critical later





1. THE SCANNER – NON-FUNCTIONAL FEATURES

- **The product should be user-friendly:**
  - Doesn't ask useless questions (like: What should I do with this malware?)
  - Doesn't overload the user with non-actionable information, unnecessary configuration options
  - Doesn't use an "Expert Mode"- isn't everybody an expert ?!
  - Doesn't expire ! We'll talk more about this later.
  - Doesn't assume YES at every question the installer might ask ☺

2. GDPR-CONFORM TELEMETRY

- Telemetry – a collection of statistical information from each endpoint running your product:
  - Installations, Uninstallations, Errors
  - Conversions from Free to Paid
  - Malware found, removed or not
  - Licensing issues, Stability of the product
  - Geographical distribution of the customers
  - Various usage statistics
- GDPR: General Data Protection Regulation has 7 principles or rights and a lot of other requirements on how to deal with the data...
- This makes telemetry really, really challenging. But not impossible!
- It gets easier with “Anonymous” Telemetry/statistics:
  - no PII: IP addresses, names, addresses, usernames, serial numbers, etc.
  - you can still calculate geographical distribution
- If you think you need these, hire a DPO

3. TESTING AND CERTIFICATION

- Several independent companies performing detection, protection, live malware removal tests
- Depending on the test type, they can test On Demand, On Access, complex scenarios (simulating a real user behavior), continuous detection
- False Positives *do* matter (in a negative way)
- Two types of tests:
  - public tests are published and advertised globally
  - private tests: usually same test configuration as the public tests, only that the results are kept private (even if they pass!)
- The big question these companies are asking:
  - Is my product as good as the product of my OEM vendor ?
  - It depends... Usually, they have additional detection & protection tech in their products

3. TESTING AND CERTIFICATION

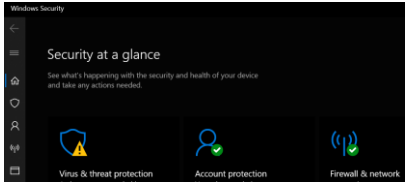
- All testing organizations offer various types of certificates/seals, which can be used in marketing activities for the product and for proof towards Microsoft (more on next slide)
- Parts of tests are outside of AM space:
  - performance: open file, download file, etc.
  - impact on the host: CPU, Memory, HDD usage, system load
  - documentation
  - usability
  - app “cleanness” and compliance
  - fairness in usage

Advice:

- Define your goals, choose carefully what you want to have tested, choose your tester and communicate with them all the time
- Look for links at the end of the presentation

4. INTEGRATION WITH THE WSC

- Windows Security Center is the security hub of Windows since Windows XP
- An AM product must register with WSC in order to become the active AM on the machine (vs. Defender or other AM)
- Functionality provided via a private API provided under NDA
- The usage changed with Win10 19H2: ELAM driver and Protected Service are required. Reason: more security needed



4. INTEGRATION WITH WSC

- How to get access to the private API ?
- In order to obtain this API you must become a member of the Microsoft Virus Initiative (MVI) (see links at the end)
- Requirements (for young companies!):
  - Offer an antimalware product developed using an SDK from other MVI partners (because you don’t implement the engine ;))
  - Have the product certified through independent testing
  - Be active in the AM industry
  - Adhere to program requirements for antimalware apps
  - Submit your app to MS for periodic testing
- The application for membership is a bit overwhelming (a lot of questions)
- There is a lot more to talk about these...

4. INTEGRATION WITH WSC

Challenges:

- No testable AM product (from the beginning)
- Apply to MVI without having all prerequisites met
- They don’t even know about MVI

- MVI will engage with these companies in a detailed conversation if they provide proof
  - that they license the SDK of an MVI member
  - that the AM product detects and removes malware successfully (via independent testing)

5. GO TO MARKET STRATEGY

- Hard time to identify and then target a market:
  - your current user base
  - localized markets: language, region, requirements
  - certain distribution channels: online searches, stores, etc.

Advices:

- Measure continuously and if needed, pivot :
  - Monitor the user base growth, the churn rate
  - Create funnels: track the lifecycle of your product and users

5.1 REPUTATION

- Keeping a good reputation is easily said than done:
  - They must produce revenue
  - Add new users, reduce churn, keep a high renewal rate
  - Keep costs under control (online user acquisition is expensive)
- What happens often:
  - bundle with various software that pays per install or install 3rd party software without explicit permission
  - yearly renewal at much higher prices
  - **the most critical**: trick users to pay using scare tactics, pay to see results, pay to fix issues

Advices:

- **Don’t forget that:**
  - There are plenty of (probably better) alternatives to your product
  - Many competitors will quickly flag your software (PUA, Adware, etc.)
- **Think long term (reputation) not short term (quick money)**

5.2 FLAGGED – NOW WHAT?

What can you do if your product got flagged by AM products ?

Determine why:

- Check the reasons mentioned in Reputation
- Verify each vendor's own set of guidelines for clean software and PUA/Adware (fortunately, the industry makes efforts to unify them)

Your only choice is:

- Fix the issues
- Contact each vendor that flagged you individually and show evidence of the fixes
- Repeat

WARNING: Not all vendors will react and not all will revert!

Better stay clean to avoid being flagged.

5.3 FREE?

- AM is becoming a commodity, just like the seatbelts and airbags for cars
- There are plenty of good “free” AM products on the market
- ... And there is also Windows Defender ...
- Due to how WSC works, a product should never EXPIRE, because it will be replaced at some point with Defender : offer a form of free product instead
- Nothing is really “free” – users pay indirectly by submitting data, seeing ads, installing advertised software
- Conclusions:
  - Home users: offer a “free” product with paid versions
  - Corporate: free makes probably no sense because of other requirements

INSTEAD OF CONCLUSIONS

- It is not enough to have good software developers and a good engine to create an AM product
- Think long term, not short term
- If you use tricks to make quick money, you will spend them all later to clean up your reputation
- In case of doubt, ask your vendor for advices

THANK YOU!

Q&A

Sorin Mustaca, www.mustaca.com

LINKS

MVI: https://docs.microsoft.com/en-gb/windows/security/threat-protection/intelligence/virus-initiative-criteria

Testing: virusbulletin.com, av-test.org, av-comparatives.com, icsalabs.com, westcoastlabs.com, skdlabs.com, check-mark.com, etc.

Cleanness: appesteem.com, CleanApps.org, CSA

Organizations: amtso.org, wildlist.org,eicar.org

GDPR: gdpr-info.eu

Disclaimer: No guarantee that the above lists are complete