Endpoint
Cybersecurity
GmbH

One year later : Challenges for young anti-malware products today

Sorin Mustaca

www.Endpoint-Cybersecurity.com

About Endpoint Cybersecurity

- About me
  - Started to work in security at RAV Antivirus more than 20 years ago, I worked at Avira (11 y) in various roles and at Honeywell in IoT security
- In 2015 founded my own company – now called “Endpoint Cybersecurity GmbH”
- Focused on three areas:
  - Consulting: help companies build better AM products and integrate security technologies
  - Create OEM endpoint security products
  - Cybersecurity services for classical infrastructures and automotive:
- Please visit www.endpoint-cybersecurity.com for additional services and more details

Why a „one year later“ presentation ?

- At the VB Conference last year I presented “Challenges for young anti-malware products today”: the difficult journey young and unexperienced companies have, when building and releasing their first AM product
- The experience I present here comes from 10 AM products analyzed.
  - 5 of my customers who are building AM products (data from The Good) and
  - 5 different AM products, I’ve never heard before, found advertised on various portals (data from The Bad). There were more initially, but I selected only those not reported as Deceptors by Appesteem.

A reminder from last year

- AM is becoming a commodity
- There are many vendors, established and new, and plenty of “free” AM products on the market (observe the “free” –> nothing is free)
- It is not enough to have good software developers and a good engine in order to create an AM product – you need special know-how, time and money to build AM products
- Think long term, not short term: if you use tricks to make quick money, you will spend them later to clean up your reputation
- ... And there is also Windows Defender ...

Agenda

- Current situation on the AM Market
  - Status of established vendors
  - Status of young vendors
  - Comparison
- Current status of the new AM products
  - Offering, Certification, Compliance
- What about Microsoft Defender?
- Conclusions

Current situation on the AM Market
Established vendors

- Established vendors:
  - Already known on the market because of their history of antimalware products
  - Are trying now to diversify their offers by adding more than just antimalware:
    - VPN, Password manager, System optimizer, Driver updater, ...
    - Online identity monitoring, File reputation, Web filters, ...
    - ... and many more
  - They mix these features into various packages, while offering them also as standalone products
  - Is this a good strategy? I let you decide.
  - Keep in mind that:
    - competition is very high, the prices for these packages need to be low
    - it is hard to differentiate these products (“my VPN/System optimizer is better than yours” ?)
    - any “extra” is adding also an “extra” load on the system (think at the big Security Suites out there)

Current situation on the AM Market
New vendors

- New vendors:
  - Very few are known on the international markets because of big marketing budgets, but most are known only in local markets or not at all
  - They are just trying to identify niche markets, determine and experiment which are the right features for their product
  - They are trying now to enhance the antimalware product the same way as the established vendors do (adding extras)
  - In the “entry level” there are usually only the core features
  - Competition on this level is even higher and the prices need to be even lower
  - Here, at the entry level, it is much harder to differentiate

Comparison

	Established vendors	New vendors
Already have users	Yes, due to history	Some do, from other products
Have several packages	Yes, bundles with other products/functionalities	Usually not, some try to upsell other products in webshop
Have own standalone products	Yes, many types	Usually not, some try to upsell other products
Have various certifications	Yes	Usually, the mandatory one for MVI, rarely more
Performance	Good, but could be better if there weren‘t all other additional mechanisms*	Very good, because they have usually just the core functionality
Detection	Very good, usually enhanced with additional functionalities	Very good, because it is based on proven OEM detection engines
Prices	High, the name and reputation matters plus the extras	Low to Medium, because they don‘t have many features and are new on the market
Target customers	All have B2C All have B2B with very few exceptions	All have B2C All want to build B2B or have already built
Free?	Some have free solutions All have a free trial (7-30 days)	Very few have a free solution All have various flavors of a free trial (7-30 days)

Current status of the young AM products
The BAD

- A few new AM products try to do a lot to become „known“ to consumers (or victims?):
  - maintain so called individual „Antivirus guides“ under different shadow companies, where their product(s) is/are on the first place(s), in the detriment of AM products (established and new)
  - work with shady affiliates that will do anything to get a click, a download or an install
  - pay questionable printed and online magazines for artificial good reviews
  - start with a very small price in the first year to increase it several times after that
- There is a huge fight on ads for keywords containing „antivirus“ -> top places are some of the above new AMs – big business for Google !
- According to Appesteem* (Aug 21st):
    - over 400 Deceptors active
    - over 200 Deceptors resolved
  - *: most these Deceptors are not AM products. It is not possible to filter after product type.
  - *: same program was added several times (with different versions)
- „Free antivirus“ has become synonym for „free download“ or „free installation“, but after that the concept of „free“ becomes quite blurry

Current status of the young AM products
The GOOD

- Fortunately, the vast majority of the new AM products
  - are solid and performant
  - have clear messages towards the user about what is free and what is not
  - do what they promise
  - are not Deceptors
  - are not promoting dumping prices for first year to increase them several times after the first year
- To be and stay „clean“ is not easy for the young companies:
  - many find out the hard way that this behavior tries to be regulated
  - costs a lot more than to add tricks for selling
  - doesn’t bring much revenue quickly
- BUT ... it pays to be “clean” over a longer time
  - New products appear all the time and more will come !
  - On the “Consumer AV Software Providers for Windows” from Microsoft, appear new vendors all the time (some of them are my current and ex-customers)

Certifications - Overview

- Last year, I explained that for new AM companies it is mandatory to be member of the Microsoft Virus Initiative (MVI) in order to be able to integrate with Windows Security Center (private API)
- To become a member of MVI, it is required to :
  - have a 3rd party AM certification of the detection capabilities and,
  - since August 2020, review by the Defender Team
- After they get admitted in MVI, they need to become L1 certified and be retested at least quarterly:
  - pass the performance test: means be “comparable” with Defender in performance (20% off is admitted) -> this is not always easy, depends on certain features!
  - test against the pre-release updates of Windows using Update Staging Lab(**USL**) or Security Update Validation Program (**SUVP**)

Certifications - Detection

- 3rd party AM certification of the detection capabilities
- Still, many young companies think that it is enough to pass the tests if the
  - hire good or many developers and
  - license a good AM engine
- Very wrong because some fail:
  - in simple On Demand tests: wrong configs, deal wrong with scan errors, archive bombs, deeply embedded objects, etc.
  - in real life tests: don’t scan downloaded files
  - due to bugs in the products
  - by detecting only platform specific malware when the tester expects cross platform detection
  - by not using properly cloud services and failing to detect fresh malware
  - by whitelisting certain code signing certificates, which are used to sign also malicious files
  - by misconfiguring own features, which have negative effects on detection: webfilters, firewalls, anti-ransomware technologies, etc.

Certifications - Compliance

- Internal compliance requirements:
  - respect the legal requirements of the engine vendor
  - add licenses and disclaimers for all used open source licenses
  - add own EULA and Privacy Agreement
- Third parties with compliance requirements:
  - respect Microsoft's engineering guidelines and contractual clauses (e.g. MVI)
  - respect Appesteem's guidelines for not getting flagged
  - respect all other vendors' requirements for not getting detected as PUA or malware by their engines
  - respect requirements from various Clean Apps groups

Conclusions #1

- Developing AM software is hard and requires experience in many areas like
  - Software Development: know how to develop a good product
  - Dev Ops: set up backends like cloud services, update servers, load balancers, testing labs
  - Compliance: understand legal language and requirements
  - Marketing: understand and create a marketing plan, create documents
  - Sales: understand how to sell a product, create and manage channels
  - Security: make the product secure by design, default, deployment
- Certifying AM software requires special skills and knowledge, and it is also expensive and time consuming
- Having a good, certified and “clean” AM product, does not guarantee market success
- The “checklist” with features comes always later - all young AMs lose here because of lack of extra features
- Very few customers are interested in non-functional features like “speed”, “reduced resources consumption (RAM, disk, CPU)”, good detection. They expect these from all products equally ☺

Conclusions – Defender

- Microsoft enforces all AMs to be at least as “good” as Defender in areas like:
  - Detection -> ensured by the 3rd party AM test and the test done by Defender Team (assumed)
  - Performance -> all AM products are required to test quarterly and be not more than 20% below Defender
- In the last tests, Defender was much better than many AM products, receiving “AV-Test Top product” and “AV-Comparatives Advanced++” several times
- **Since Defender is free and “good”, why bother with free and paid AM products then?**

Final Conclusion: is it worth in the end?

- *Here are my thoughts why companies will keep building AM products:*
- Defender has perception problems:
  - people don't want to protect the OS with AM from the same vendor. Remember: "they write the viruses and then sell the antivirus" ?
  - the performance hasn't always been so good as now – this might change the perception over time!
- The extras included in (some of) the AM products are making a difference
- The extras included in paid AM bundles get cheaper in bundles (just perception, not facts)
- "try before you buy" : try in consumer before buying the enterprise version
- Usually customers get a better support from the ISVs than from Microsoft
- Data sharing is "simpler" with smaller ISV
- The "Buy local" concept is real and it works
- Users are easier attracted to try AM products by receiving a solution when they find it at the right moment (messaging by using advertising)

Thank you!

Sorin Mustaca

sorin@endpoint-cybersecurity.com

www.endpoint-cybersecurity.com

~ Build your own antimalware ~