Why “in-the-cloud” scanning is not a solution

Andreas Marx, Maik Morgenstern
AV-Test GmbH, Magdeburg, Germany

http://www.av-test.de
Disclaimer

• This presentation is not meant to bash in-the-cloud technologies nor the vendors that implement and use those.

• This presentation is merely a reaction to the marketing hype, that tries to praise in-the-cloud technology as the holy grail of anti-virus software.

• This presentation is going to put a few things into perspective.
Content

• Theoretical Aspects
• Testing Experiences
  – The cloud doesn’t know more than others
  – The cloud is slow
  – The cloud is unreliable
  – The cloud is getting bigger, the local databases too?
• Conclusion
Theoretical Aspects

1. User receives new file via email or web
2. No detection with existing .DATs, but the file is "suspicious"
3. Fingerprint of file is created and sent using McAfee Artemis Technology
4. McAfee Artemis Technology reviews this fingerprint and other inputs statistically across threat landscape
5. McAfee Artemis Technology identifies threat and notifies client
6. VirusScan processes information and removes threat
7. Customer ePO updated
Theoretical Aspects

• Essentially:
  – Moving the signature databases for static detection from the local PC to the cloud
  – The protection lifecycle pretty much remains the same, only the way of deploying updates changes
  – New points of failure are introduced, when depending on a working internet connection to identify threats
  – Instead of developing new protection technologies, the existing ones are stressed to the maximum, which doesn‘t solve any problems, but only delays them a bit
Testing Experiences

• The cloud doesn‘t know more than others
  – In-the-cloud products are not automatically #1 in our tests
  – A lot other products are as good or even better without any cloud
Testing Experiences

• The cloud doesn’t know more than others
  – Detection rates are very similar for the top products, no matter if a cloud is used or not
  – The top six products in our CollScan test are ranging between 99.97% and 99.77%
  – Only two of those six very good products (in regard to static detection) use in-the-cloud scanning, four others don’t
  – Top ten products are all above 99% and even the top 20 are all above 95%
Testing Experiences
Testing experiences

• The cloud is slow
  – Providing signatures through the cloud, doesn’t mean the user is always instantly protected
  – The signature itself still has to come from somewhere, the cloud doesn’t solve this problem
  – Sometimes the cloud is even slower than BETA or emergency updates of the same vendor
  – The cloud seems to be just another way of deploying updates, but not adding any additional security

A random example of many (FILE_X93f1.exe):

AntiVir: -
AVG: -
BitDefender: TrojanDownloader.Bredolab.U
Fortinet: W32/Waledac.X.gen!tr
F-Secure: TrojanDownloader.Bredolab.U
Kaspersky: Packed.Win32.Krap.w
McAfee: -
McAfee (BETA): Bredolab.gen.a (trojan)
McAfee (Online): -
Microsoft: VirTool:Win32/Obfuscator.GO
Norman: W32/Obfuscated.D2
Panda: -
Panda (BETA): -
Panda (Online): -
Sophos: Mal/Bredo-A
Symantec: -
Symantec (BETA): Packed.Generic.243
Trend Micro: TROJ_BREDOLAB.J
Testing Experiences

• The cloud is slow
  – Special test (2009-09-07 to 2009-09-18) performed for this presentation:
    • There were several samples that were only detected after 10 days after we first saw them by the inspected in-the-cloud products
    • There were samples that were never detected during our test
    • There were samples that were detected by other vendors with generic signatures or heuristics way before a cloud detection was available
Testing Experiences

- The cloud is unreliable
  - Reviewed during our test for this presentation and basing on earlier experiences
  - We have seen system outages, both due to a lagging internet connection (our fault, the vendors fault?) as well as failing servers on the vendors side
  - Detections fluctuate and when you have bad luck, you are unprotected for a while
  - Cloud detections are changed (or additionally added) to local signature detections. Are vendors not sure whether to trust their own cloud?
Testing Experiences

- Sample: 0a9a343e3d19ca7e2d9e3ac34623568c
- First seen at AV-Test: 2009-09-09

<table>
<thead>
<tr>
<th>Date-Time</th>
<th>Product A</th>
<th>Product B</th>
</tr>
</thead>
<tbody>
<tr>
<td>20090909-181853</td>
<td>-</td>
<td>suspicious</td>
</tr>
<tr>
<td>20090909-221853</td>
<td>-</td>
<td>suspicious</td>
</tr>
<tr>
<td>20090910-021853</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>20090910-061853</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>20090910-101853</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>20090910-141853</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>20090910-181853</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>20090910-221853</td>
<td>-</td>
<td>Trj/Cl.A</td>
</tr>
</tbody>
</table>
Testing Experiences

- Sample: 16c6a9860277a639f97cc21e3a59722c
- First seen at AV-Test: 2009-08-31

<table>
<thead>
<tr>
<th>Date-Time</th>
<th>Product A</th>
<th>Product B</th>
</tr>
</thead>
<tbody>
<tr>
<td>20090907-160354</td>
<td>BackDoor-EEC (trojan)</td>
<td>Trj/CI.A</td>
</tr>
<tr>
<td>20090907-200354</td>
<td>BackDoor-EEC (trojan)</td>
<td>Trj/CI.A</td>
</tr>
<tr>
<td>20090908-000354</td>
<td>BackDoor-EEC (trojan)</td>
<td>Trj/Downloader.MDW</td>
</tr>
<tr>
<td>20090908-040354</td>
<td>BackDoor-EEC (trojan)</td>
<td>Trj/Downloader.MDW</td>
</tr>
<tr>
<td>20090908-080354</td>
<td>BackDoor-EEC (trojan)</td>
<td>Trj/Downloader.MDW</td>
</tr>
</tbody>
</table>
Testing Experiences

- The cloud is getting bigger, the local databases too?
- As in-the-cloud queries are (often) only a supplement to the traditional technologies, the local databases don’t shrink (that much)
Conclusion

• We looked at in-the-cloud technologies from a static detection point of view

• We didn’t cover:
  – False positive issues
  – Performance impact
  – Attacks to the approach

• We primarily listed the bad things
Conclusion

• In-the-cloud scanning is helping the vendors to get their static detections rate up
• With reputation systems and further statistical analysis, those approaches can help even further in detection malware
• But: In-the-cloud scanning is still only a part of a whole security infrastructure
• Products that use in-the-cloud approaches are not necessarily better then other products, but they are often better than before (when they didn’t have the cloud)
Conclusion

• All in all:
  – In-the-cloud scanning can be a valuable addition to security software
  – But the cloud itself is not the solution
    • Static scanning doesn’t care where the signatures come from
    • Heuristics also work without the cloud
    • Behavior-based systems don’t rely on the cloud either
Question & Answers

Thank you very much for your attention!

Are there any questions?

Note: Many testing papers can be found at:
http://www.av-test.org → Publications → Papers