AV-TEST
Tests of Anti-Virus-Software independent • qualified • fast

Runtime Packer Testing Experiences

Maik Morgenstern & Andreas Marx
AV-Test.org, Germany

2nd International CARO Workshop, May 2008

Agenda

- Introduction
- Everything but detection rates
  - Performance
  - Blacklisting, Misdetections and False Positives
  - Security Vulnerabilities, DoS Attacks
- Conclusion

Introduction

- The majority of malware is runtime packed
- Unfortunately runtime packers are also used in legitimate applications (goodware)
- We're speaking not only about packers, but also obfuscators, encryptors, installers etc.
- These techniques have been used for many years, not a few months
- Still, runtime packers challenge AV software in many aspects

Introduction

- A few numbers to begin with:
  - About 50 different runtime packers were used in the February 2008 WildList collection, divided into lots of different versions
  - Many packers were only used in one to five malware samples
  - We received more than 20,000 samples during the period of April 19-21, 2008: about 150 different runtime packers were used (in many different versions)
  - UPX was used in more than 50%; most of the other packers were used in a small number of samples only

Everything but Detection Rates

- If you were looking for a presentation that focuses e.g. on detection rates:
  - "Runtime Packers: The Hidden Problem?" by Tom Brosch and Maik Morgenstern, AV-Test.org, presented at Blackhat USA 2006
- We'll look at other aspects of runtime packer testing experiences today

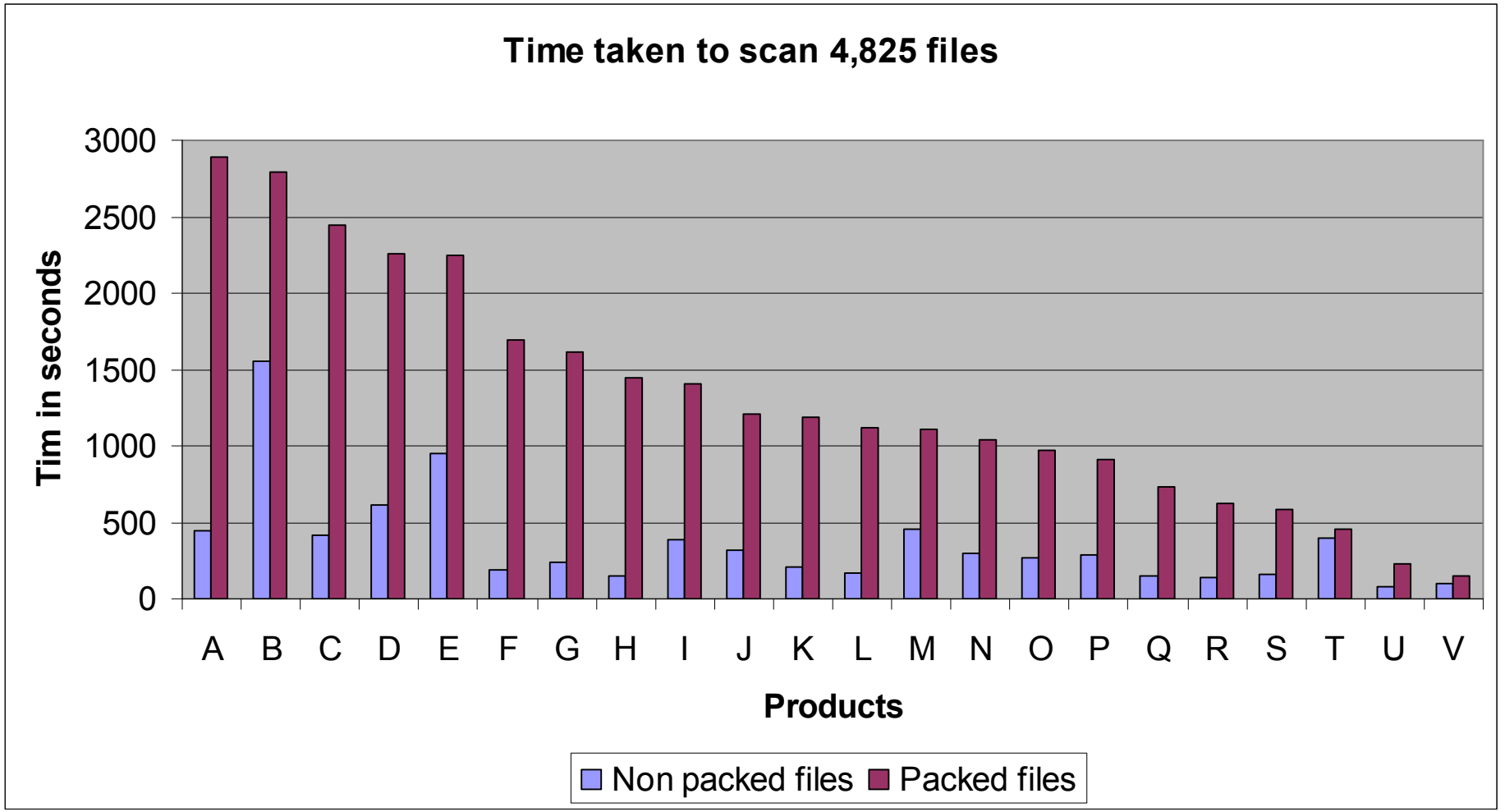
Performance

- When scanning runtime packed files, scanning performance (speed) usually decreases a lot
- Why is that?
  - Runtime packers require additional work from the scanner (check PE header, code at EP, unpacking)
  - This has to be implemented for a wide range of different packers (with various versions and packing options)
  - Alternatively, generic unpacking routines are used (which are usually slower than dedicated ones)

Performance

- What can be tested?
  - The time required to scan a set of runtime packed files vs. a set of non-packed files
  - The time required to scan files packed with a certain runtime packer vs. a set packed with a different packer

Performance



Performance

- One randomly chosen product takes the following times to scan files packed with:
  - ACProtect 1.35a: over 2 seconds
  - Armadillo 1.90: below 0.1 seconds
  - tELock 0.60: around 1 second
  - UPX 1.03: over 2 seconds
  - UPX 1.08: below 0.8 seconds
- Non-packed files: below 0.05 seconds

Blacklisting, Misdetections and FPs

- Runtime packers increase scanning times, some more than others
- Efficient way to get around this:
  - Blacklisting of (certain) runtime packers
- Blacklisting is also easier for vendors than adding full unpacking support
- However, increased risk of false positives
- Open question: which runtime packers can be confidently blacklisted?

Blacklisting, Misdetections and FPs

- What can be tested?
  - Artificial test sets:
    - Pack non-packed “good” or “bad” files with different runtime packers, with different versions, with different options
  - Real life test sets:
    - Use clean applications which include runtime packed files
- What else?
  - Results have to be interpreted
  - Especially in case of the artificial test set, not every supposedly FP is a FP
  - Some runtime packers may only (or primarily) be used in malware, so blacklisting them might be OK

Blacklisting, Misdetections and FPs

- Usage of runtime packers in malware and good applications
  - UPX is always at the top, in goodware as well as malware (far more than 50% of the files)
  - Other top ones for malware: PECompact, Upack, ASPack/ASProtect, tELock, FSG, Themida, Armadillo, MEW, Nullsoft Installer
  - Other top ones for goodware includes: Armadillo, ASPack/ASProtect, PECompact, Nullsoft Installer

Blacklisting, Misdetections and FPs

- Test results of the artificial test set (4,825 files):
  - Nearly all of the 30 tested scanners did “detect” something in the set of runtime packed clean files
  - “Detection scores” range from less than 10 up to 4,027
  - Most of these detections are just “suspicious” or some kind of “generic malware” detections
  - Most often flagged packers:
    - Exebundle 2.8 by up to 23 scanners
    - Secupack 1.5 by up to 18 scanners
    - PESpin 0.3 by up to 12 scanners
    - Armadillo 2.52 by up to 10 scanners
  - Only PESpin and Armadillo are seriously used today, according to an analysis of samples received between April 19-21, 2008

Blacklisting, Misdetections and FPs

- On the other hand, the most widely used packers in malware didn't trigger as many "detections"
  - UPX 0.90 had up to 5 detections, other versions were even lower
  - PECompact and ASPack had up to 6 detections
- What happened? Malware authors are of course catching up with the blacklisting of certain runtime packers

Blacklisting, Misdetections and FPs

- Besides blacklisting of packers there are also misdetections:
  - An Armadillo packed file is detected as Rbot, Spybot or Sdbot from different scanners
  - Some PECompact packed files are detected as Peed trojan
  - Some FSG packed files are detected as Agent worm
- Looks like some malware detection signatures need to be improved…

Blacklisting, Misdetections and FPs

- We have blacklisting of certain runtime packers, which sometimes aren't even relevant in the malware world anymore
- We have misdetections of runtime packed files, which don't contain malicious code
- Consequently one would expect false positives in real life

Blacklisting, Misdetections and FPs

- We checked out the Top 50 & Top 30 download lists at cnet.com and zdnet.de
- 4 of the downloaded installers were runtime packed (2 UPX, 1 PECompact, 1 PEncrypt) and 25 used the Nullsoft installer
- 88 of the installed files were runtime packed (71 UPX, 7 ASPack/ASProtect, 5 PECompact, 3 Armadillo, 1 tELock) and 41 used Nullsoft
- Examples are: Google Desktop, avast! Antivirus, BearShare, ICQ 6, Winamp 5.5, Ad-Aware 2007, DivX

Blacklisting, Misdetections and FPs

- Test results confirm the assumption:
  - All of the 4 runtime packed setup files were flagged by 1 up to 3 scanners with 2 signature (mis)detections and 8 suspicious or generic detections
  - It gets worse with the installed files, detections range from 0 to 5, adding up to 160 detections
  - Out of the “Top 5” products from the artificial test set, 3 make it in the “Top 5” of the real test set, with 77, 17 and 11 detections
  - Some of the programs that scored high (=bad) in the artificial test set had zero FP in the real life test

Security Vulnerabilities, DoS Attacks

- Just a few headlines from 2007 and 2008:
  - F-Secure Archives and Packed Executables Detection Bypass
  - ClamAV Upack Processing Buffer Overflow Vulnerability
  - Trend Micro AntiVirus fails to properly process malformed UPX packed executables
  - ClamAV libclamav MEW PE File Integer Overflow Vulnerability
  - Kaspersky AntiVirus UPX File Decompression DoS Vulnerability

Security Vulnerabilities, DoS Attacks

- No matter whether you do blacklisting, have dedicated or generic unpacking routines, you will always have to parse the file to some extent
- False assumptions and coding errors will then lead to exploitable vulnerabilities in the code
- An overview of such problems in security products has been given: “Insecurity in Security Software” by Andreas Marx and Maik Morgenstern at the Virus Bulletin Conference, 2005

Security Vulnerabilities, DoS Attacks

- What can be tested?
  - Real life test sets
    - How well do the products cope with runtime packed files found in the wild?
  - Artificial test sets
    - Pack non-packed files with different runtime packers, in different versions, with different options
    - Extension: Use fuzzing or similar techniques to alter the PE header or other parts of the PE file

Security Vulnerabilities, DoS Attacks

- Good news first:
  - The number of problems was small in this test run:
    - No problems in the real life test set
    - Only two scanners had problems with the artificial test set, one crashed while scanning ASPack 2.11, another one crashed on ACProtect 1.41
- Bad news:
  - This wasn't the first or the last time we came across such problems
  - There are always other people who will find more issues

Security Vulnerabilities, DoS Attacks

- So what to do?
  - Enforce secure coding practices (this also means reviewing old code)
  - Extend your test sets, include all the runtime packers you can find and use all the versions and options that are there
  - Use fuzzing technologies, even if that renders the PE file invalid, it may still point to problems

Conclusions

- Blacklisting:
  - Helps with solving performance issues, but introduces the risk of false positives
  - List of blacklisted runtime packers needs to be constantly reviewed and updated to minimize the risk of false positives and to be effective
  - Also decreases the risk of exploitable vulnerabilities, since less and easier parsing work is required

Conclusions

- Dedicated unpacking routines:
  - Good way to get around false positives, unpack the sample with the dedicated routine you have and match a signature
  - Usually slower than blacklisting, but faster than generic routines
  - Lot of work required to keep up with the different runtime packers, new ones need to be added, old ones need to be updated, this introduces a lot of code which can contain vulnerabilities
- Generic unpacking routines:
  - Are a nice way to deal with the many different (even unknown) packers out there, but are usually the slowest option
  - The codebase might be easier to maintain, especially in regard to vulnerabilities, since changes are less often necessary than with dedicated unpacking routines

Conclusions

- No matter what technique is being used in a product, there will always be problems (read: challenges)
- The work is never finished, updates and changes are always required. Not only with new runtime packers evolving, but also with the usage changes of those in malware and in goodware

Thanks for your attention!

Many testing papers and related documents can be found at our website http://www.av-test.org