

Runtime Packers: The Hidden Problem?

Tom Brosch, Maik Morgenstern
AV-Test GmbH



Contents

- Motivation – What is the Problem?
- Issues involved – Our Testing results
 - Detection Rates
 - False Positives
 - Crashes and other Problems
- Conclusions



What is the Problem?

- How many of the Malware files out there are runtime packed?
 - WildList 03/2006: Over 92%
 - Only 54 out of 739 files are not packed
(According to a quick analysis with PEiD and manual review)
- About 30 different Packer/Crypter are used
- Some of the top ones:
 - UPX: 167 files
 - Morphine: 72 files
 - MEW: 59 files
 - FSG: 50 files
 - PESpin: 32 files



What is the Problem?

- A review of some common Malware families:
 - Bagle: 62 out of 63 files are runtime packed. 5 different Packers, in 7 different versions have been used
 - Mytob: 241/246. 20 Packers, in 32 different versions
 - SDBot: 58/58. 12 Packers, in 16 different versions
- Observation:
 - Nearly every Malware is runtime packed
 - Many different Packers are used throughout one Malware family to avoid detection
- Conclusion:
 - Anti-Virus Software needs to deal with a lot of Packers and be prepared for new ones every day



What is the Problem?

- Nearly all AV products employ Unpacking engines. So everything is fine? Well, no! Why? The engines have many flaws, aren't generic and have a hard time keeping up.
- There is a lot of activity in research in this area:
 - *Defeating polymorphism: beyond emulation*, Adrian E. Stepan (Microsoft), Virus Bulletin Conference 2005
 - *Generic unpacking – how to handle modified or unknown PE compression engines?*, Tobias Graf (Ewido Networks), Virus Bulletin Conference 2005
 - *Unpacking - a hybrid approach*, Vanja Svajcer, Samir Mody (Sophos), Eicar Conference 2006
- Detection rates are not great anyways:
 - Microsoft: 41%
 - Ewido: 73%
 - Sophos: 30%



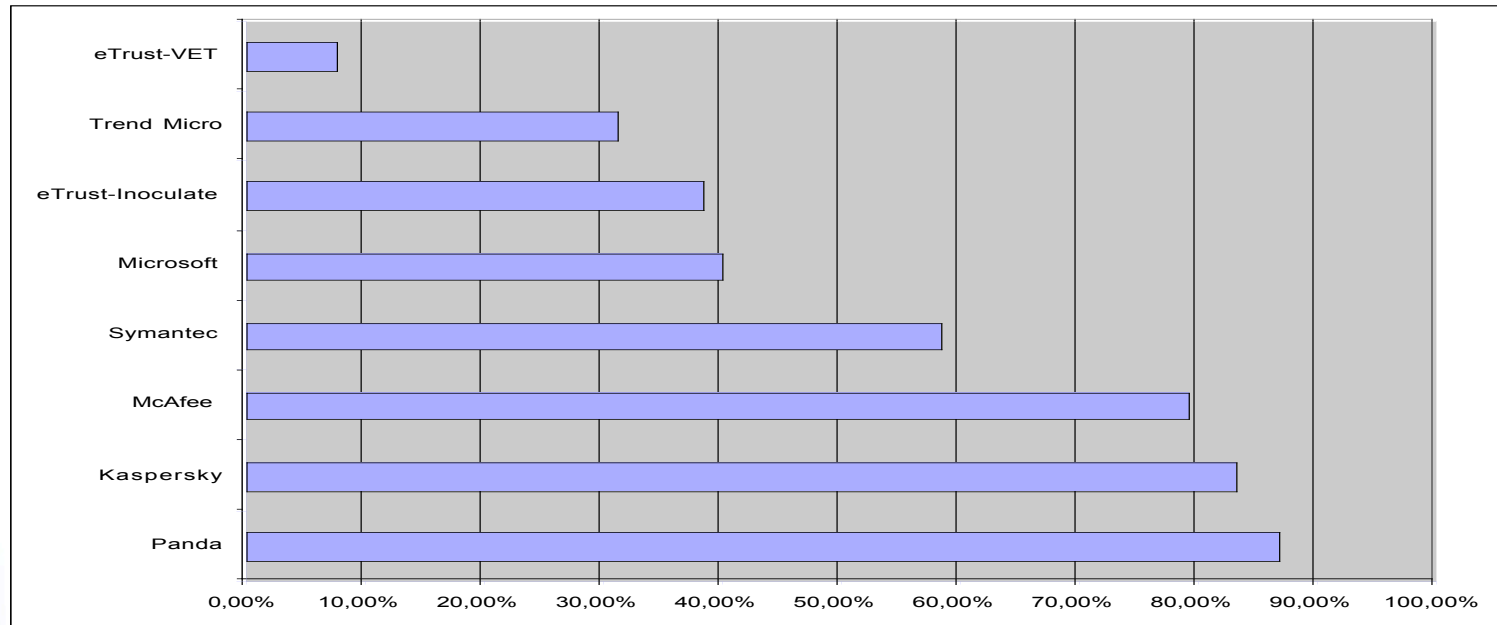
Testing Results

- Used Testsets and Testsetup
 - Malware Testset: 10 common Malware files, packed with about 40 different Runtime Packers in over 500 versions and options: Over 5000 files, **2941** still running correct which were used for the test
 - Falsepos Testset: 10 clean files (Windows and standard applications), packed with the same options as above
 - For Details of used Packers and Versions see additional material
 - Testsetup of Anti-Virus products:
 - 27 Commandline Versions in an automated environment
 - 7 GUI Versions tested manually on Windows XP SP2 (English)
 - Latest Updates and signatures from around June 20th, for exact Versions used see additional material
 - On PIV 2.8GHz, 512MB, 40GByte HD



Detection Rates

- Malware Testset Results range from 10% to over 80%
- But: Be prepared for False Positives on several products



Detection Rates

- Packers used in WildList Malware
 - Interestingly the products perform pretty good (nearly always over their own average) on Packers used in WildList Malware
 - But they perform usually worse on Packers not used in WildList
 - Many Packers aren't detected at all by some products



Detection Rates

- Top 5 Packers in WildList:

	Kaspersky	McAfee	Symantec	Microsoft
Average on the Malware Testset	83%	79%	58%	39%
ASpack	95%	97%	95%	81%
FSG	100%	100%	56%	100%
Morphine	100%	70%	100%	0%
UPX	96%	97%	92%	100%
MEW	100%	86%	53%	80%



Detection Rates

- „Bad“ performance on others Packers:

Kaspersky	McAfee	Symantec	Microsoft
Armadillo: 6%	Armadillo: 14%	Acprotect: 33%	ASProtect: 26%
ASProtect: 80%	Obsidium: 18%	Exe32pack: 18%	PEBundle: 14%
PEBundle: 81%	yodas Protector: 55%	Neolite: 22%	PECompact: 24%



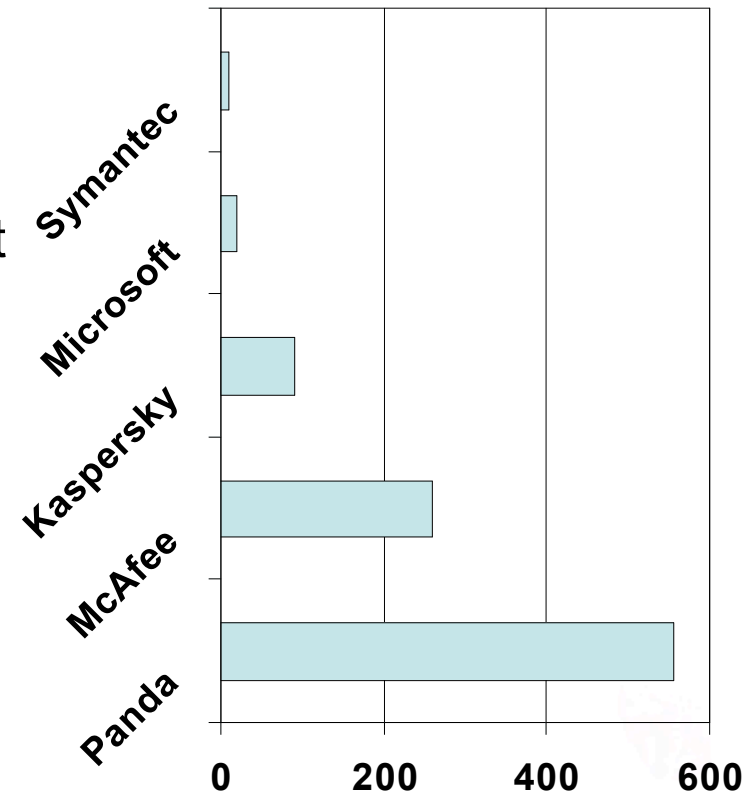
Detection Rates

- Packers not detected at all
 - Microsoft: Armadillo, Krypton, Obsidium
 - Symantec: Armadillo, ASProtect, Shrinker
 - McAfee: Epack, PELock
 - Kaspersky: SVK-Protector
 - TrendMicro: Acprotect, Armadillo, Cexe



False Positives

- “Suspicious” problem:
 - Panda had good detection rates (86%), but with a lot “suspicious” (because the Runtime Packer got flagged), which in turn results to many False Positives (556) now, since the Packer gets flagged again. The same issues occurred on eSafe and Fortinet with 2091 resp. 1854 False Positives for example.



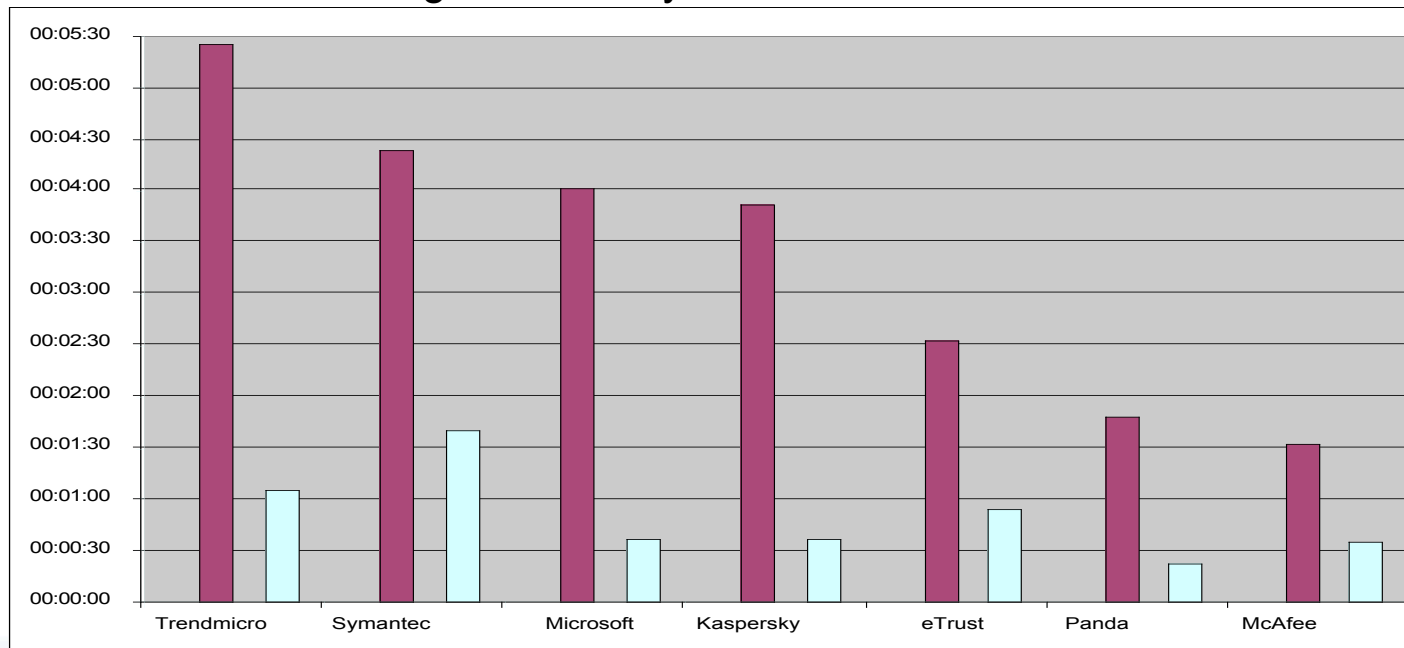
False Positives

- Only TrendMicro and eTrust triggered no False Positives
- Other products ranged between ten and several hundred up to 2091 as seen before
- Common False Positives:
 - Exebundle gets flagged as malicious by McAfee, Microsoft, Kaspersky and Panda
 - Many Scanners wrongly flag packed files as certain Malware
 - Kaspersky for example flagged several Armadillo packed files as Backdoor.Win32.Agobot.afn or Backdoor.Win32.Rbot.ip



Crashes and other Problems

- Scanning speeds
 - Dr.Web took around 20 seconds on 2941 non packed files, but over 2 hours on the same files packed, TrendMicro 1 minute vs. 5 minutes
 - Increase in scanning time usually between the factor 1.5 and 10



Crashes and other Problems

- Two of the problems we faced in our test:
 - Panda GUI Version:
 - When scanning certain files packed with Cexe Packer, the scan simply stops at that file without any error
 - So just place the Cexe ahead of your malicious files and they won't be scanned
 - TrendMicro Commandline Scanner:
 - When scanning certain files packed with Petite, the scan will stall
 - Easy DoS possible if you „accidentally“ send a file like that to an E-Mail Gateway using TrendMicro products
- For other problems in Security Software see: *Insecurity in Security Software*, Maik Morgenstern, Andreas Marx (AV-Test GmbH), Virus Bulletin Conference 2005



Conclusions

- Three main issues:
 - Detection Rates: Detection of Packers commonly found in the WildList is OK, Detection of other Packers still needs to get a lot better!
 - Falsepos: Nearly all products trigger False Positives and some just flag many packed PE files as “Suspicious“. Also several False Positives were detected as a certain Malware which might indicate bad signatures.
 - Crashes/Speed problems: Scanning packed files increases scanning times and the system load a lot. Also some Scanners had serious problems when scanning packed files. We had the Archive problems last year, so can we expect Runtime Packer Problems next year?



Conclusions

- Proposals:
 - AV Vendors need to support Runtime Packers not found in the WildList, else virus writers will just switch to yet undetected Packers
 - Of course it's not possible to catch every Packer (Version) out there, so heuristic or generic approaches should be combined with the dedicated unpacking engines
 - But some heuristic approaches need to get a lot better than just flagging all packed PE files
 - Also signatures need to be more carefully chosen to avoid False Positives that way
 - Possible problems in unpacking engines should be reviewed and removed to avoid the issues we have seen with archives last year



The End

Thank you for your Attention.
Any Questions?

Tom Brosch, Maik Morgenstern
www.av-test.org

