TASK
TORONTO AREA SECURITY KLATCH
WWW.TASK.TO

The Failure of Anti-Virus Software (?)

Prepared By: Robert W. Beggs, CISSP CISA
25 OCtober 2006

DIGITAL DEFENCE

Introduction

- Robert Beggs, CISSP, CISA
  - 15+ years experience in Information Security
  - Military, biomedical research, consulting, financial services background

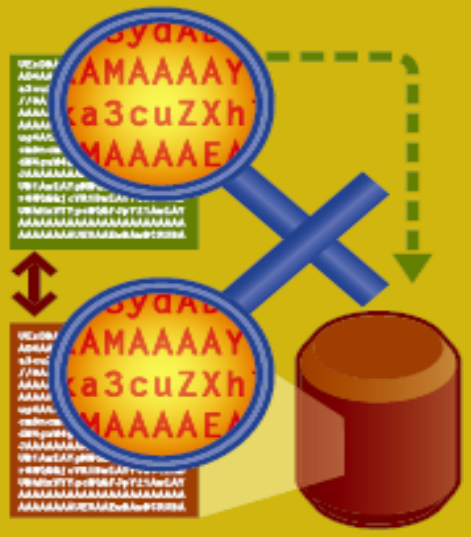
- DigitalDefence
  - **9-1-1 for Data Security Incidents**
  - Focus on providing incident management services (prevent, detect, respond)
  - Target Canadian enterprises

State of the Nation …

- 100,000 – 180,000 viruses believed to exist “in the wild”
- “Infinite amount” in virus zoos
- At least 250 new malware programs (worms, Trojans, spyware, hacker tools) released per day
- To stop them, we use AV software …

http://www.gfi.com/documents/rv/msecpcmag04.pdf

SIGNATURE

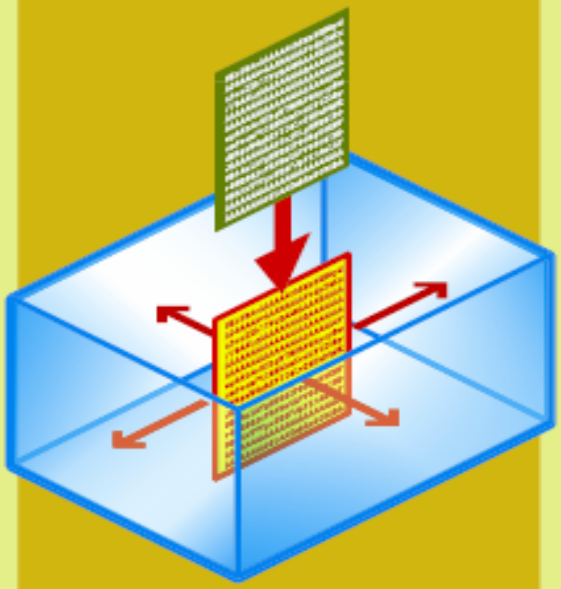


A traditional antivirus program uses *signatures*—byte strings unique to specific viruses—and compares the code being scanned against the signatures in its database.

HEURISTIC

Heuristic virus detection involves scrutinizing the code to find indications of suspicious activity. For example, does the code delete files, change the Registry, or format drives?

SANDBOX



Sandboxing lets programs, including viruses, run in an area sequestered from the rest of the system. If a program does something untoward, the antivirus utility shuts it down.

DIGITAL DEFENCE

State of the Nation …

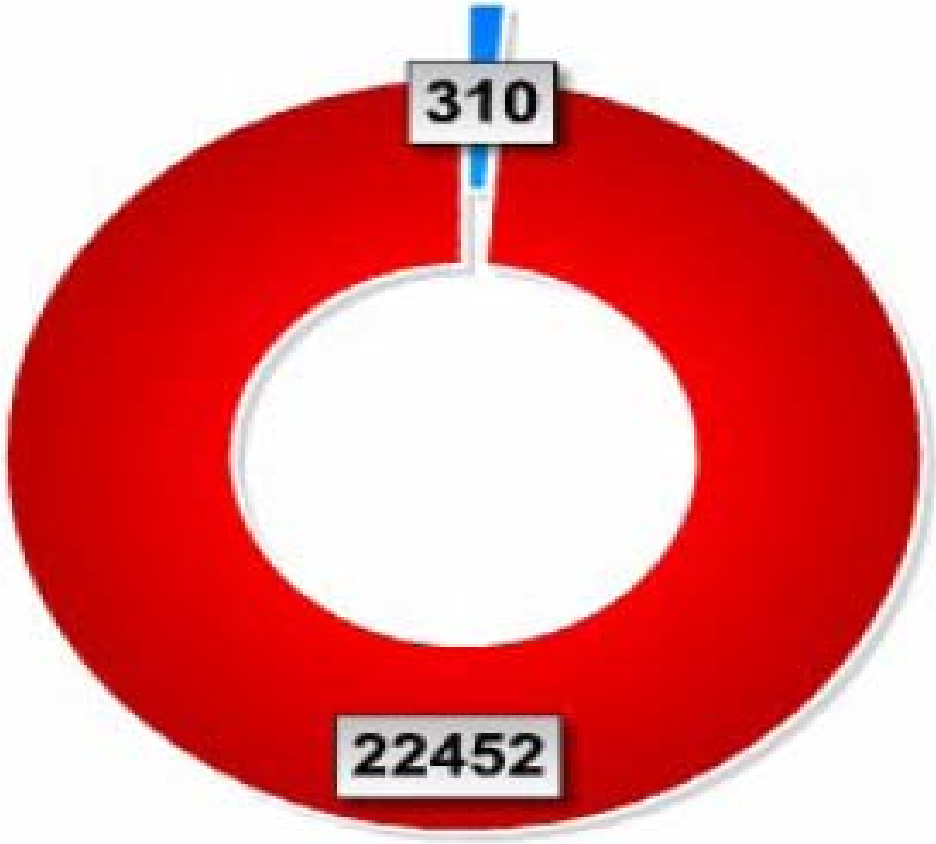
- AV software is primarily signature-based – examines software for the “signature” of a known virus
- It’s worked for 20 years, right?

Limitations of Signature-Based Scanners

- No common definition of “malware”
- Collections of malware biased according to collection method; no common repository
- Signatures reactive; out of date
- Attackers write code to beat top AV software
- “Queen Bots” (Paul Vixie and David Dagon, BH06)
  - Repacks bot with new key, multiple packers
  - Dead / random code (“polymorphism”)
  - Automated randomization of signatures
- Is this really a problem?

7 Day Analysis (Virustotal.com)

Uses 20+ AV engines to analyze suspect malware



Blue: Infected files detected by all antivirus engines.
Red: Infected files not detected by at least one antivirus engine.

DIGITAL DEFENCE

Issues #2 – Response Times

(http://www.gfi.com/whitepapers/why-one-virus-engine-is-not-enough.pdf)

Table 1 – Response times of anti-virus companies to the outbreak of w32.Sober.C

Company	Time to respond in hours (closest half hour)
BitDefender	10.5
Kaspersky	12.0
F-Prot (Frisk)	12.5
F-Secure	13.0
Norman	15.5
eSafe (Alladin)	15.5
TrendMicro	17.0
AVG (Grisoft)	17.5
AntiVir (H+BEDV)	19.5
Symantec	25.0
Avast! (Alwil)	31.0
Sophos	35.5

McAffee = 49 hours !

DIGITAL DEFENCE

The Consumers Report Test (2006)

Expert • Independent • Nonprofit
ConsumerReports.org®

- Created 5,500 new virus variants derived from six categories of known viruses, “the kind you’d most likely encounter in real life”
- We infected our lab computer with each of 185 of them to see whether the products could better detect viruses that were actively executing, based on their behavior
- Scanned more than 100,000 clean files (false positives)
- The AV industry freaked!

Consumer Reports Redux …

- Ethics and morality of “creating a virus”
- Created 5500 viruses, used 185 per test bed – the same 185? (consistent methodology problem)
- Consumer Reports tested antispyware applications – but they *did not test against any spyware for their antispyware testing*
  - Instead, their *entire* test of antispyware applications was based on running applications against Spycar, a set of applications that mimic spyware behavior (http://sunbeltblog.blogspot.com/2006/08/consumer-reports-testing-scandal-its_25.html)

So, How Do You Test AV Software?

- On-demand testing
- **NOTE: Due to copyright restrictions, data from AV Comparatives is NOT presented directly in this report**
- For the most current data, go to: http://www.av-comparatives.org/

DIGITAL DEFENCE

But How Do We Detect New Viruses?

- Retrospective testing
- Take AV software that's up-to-date; make an image on a defined OS platform
- Lock the image away for 3 months ("yesterday")
- Take it out ("today") and reinstall image
- Test it against malware that is current "today"
- The % detection = how good "yesterday's" AV software was at detecting zero day threats
- No need to write new viruses!

Let's Try Retrospective Testing …

- **NOTE: Due to copyright restrictions, data from AV Comparatives is NOT presented directly in this report**
- For the most current data, go to: http://www.av-comparatives.org/
- You will find that the virus detecting ability drops from 90%+ to as low as 7% when you perform this testing → AV software based on signature recognition is not very good at detecting zero-day malware!

References

- www.virusbtn.com
- www.av-comparatives.org
  - Review their methodology, and results
  - When I post this presentation, will only link to their data
- www.wildlist.og
  - The viruses that are really spreading in the wild
- http://www.av-test.org/
  - Cross-reference of virus names used by vendors
- http://www.mcafee.com/common/media/vil/pdf/imuttik_VB_conf_2001.pdf
  - Good overview of testing methodologies, failure of using incomplete testing sets

The Canadian Information Security Newsletter

- FREE information to Information Security and Privacy specialists
- Canadian-focused
- Provides information on:
  - Upcoming events, conferences
  - Feature articles, items of interest
  - Canadian security and privacy news items
- Subscribe at:
  - www.digitaldefence.ca\subscribe

Contact


DIGITAL
DEFENCE
Robert Beggs
President
First Canadian Place
100 King Street West, 37th Floor
Toronto, ON M5X 1K7
Phone: (416) 306-5775
Mobile: (647) 444-1492
Fax: (416) 644-8801
email: robert.beggs@digitaldefence.ca
web: www.digitaldefence.ca