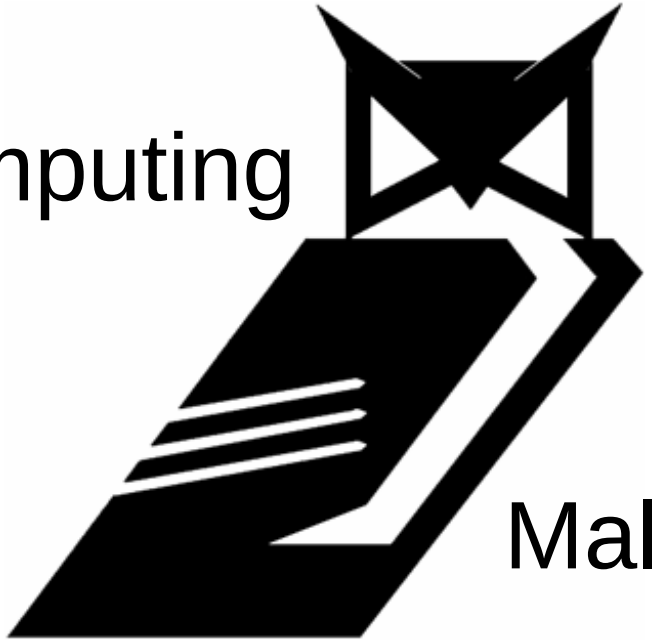
Offensive Computing



Malware Secrets

Valsmith (Valsmith@offensivecomputing.net)

Delchi (delchi@offensivecomputing.net)

Valsmith

BACKGROUND:

Malware analyst
Penetration tester
Exploit developer
Reverse Engineer

AFFILIATIONS:

OffensiveComputing
Metasploit
cDc/NSF

Delchi

BACKGROUND:

Incident Response
Intrusion Detection
Data Mining / Log Correlation

AFFILIATIONS:

OffensiveComputing
cDc/NSF

What is this?

- Offensive Computing
  - What we do
- Database
- Findings
  - Packers
  - AV statistics
  - URLs
  - Other Interesting Data
- Future
- Questions

Offensive Computing

- Malware Blog
  - Posts from OC members and community
  - Interesting malware discussions
    - Rustok
    - Dolphin Stadium trojan
    - Symantec Worm / Big Yellow
- Sample Collection
  - 140,054 samples and growing
  - Available for download
- Auto-Analysis
  - Uploaded samples baseline analyzed

Database

- Database of associated malware information
  - Searchable web interface
  - File typing
  - Multiple Checksums (md5,sha1,sha256)
  - Packer detection (modified *msfpescan*)
  - Multiple Anti-Virus scan
    - Bitdefender
    - Antivir
    - Clamav
    - F-Prot
    - McAfee
    - Kaspersky
    - Avast
    - AVG
    - F-Secure
    - More coming

Database

- PE Info
    - Based on PEFile project from Ero Carrera with contributions by Danny Quist, OC
- Binary archive
- Strings
- File size
- Auto-unpacking coming soon! (see our other talk)

Findings

- Ok so we have all this malware, now what?
- Time to mine the data
- What might be interesting?
  - Packer statistics
  - Common strings
  - URL's (call back, command and control, droppers)
  - E-mail addresses
  - IP addresses

How these statistics were gathered

- Files collected via
  - Raw submissions to OC via web
  - Honeypots
  - Spam attachments
- Any file could have been uploaded
  - Including benign files, system files, etc.
- Files were NOT manually verified to be malware
  - Still useful test, AVs scan non-malware
  - Most current AV signatures used
- Linux based AV scanners only

How these statistics were gathered

- Results of auto-analysis saved in database and text files
- Analysis data mined with PERL / shell scripts
- Tool called *pizda* developed by Delchi to data mine results
- Results could be somewhat “fuzzy”
- Many genetically similar samples exist in sample set
    - Different md5sum / same basic functionality

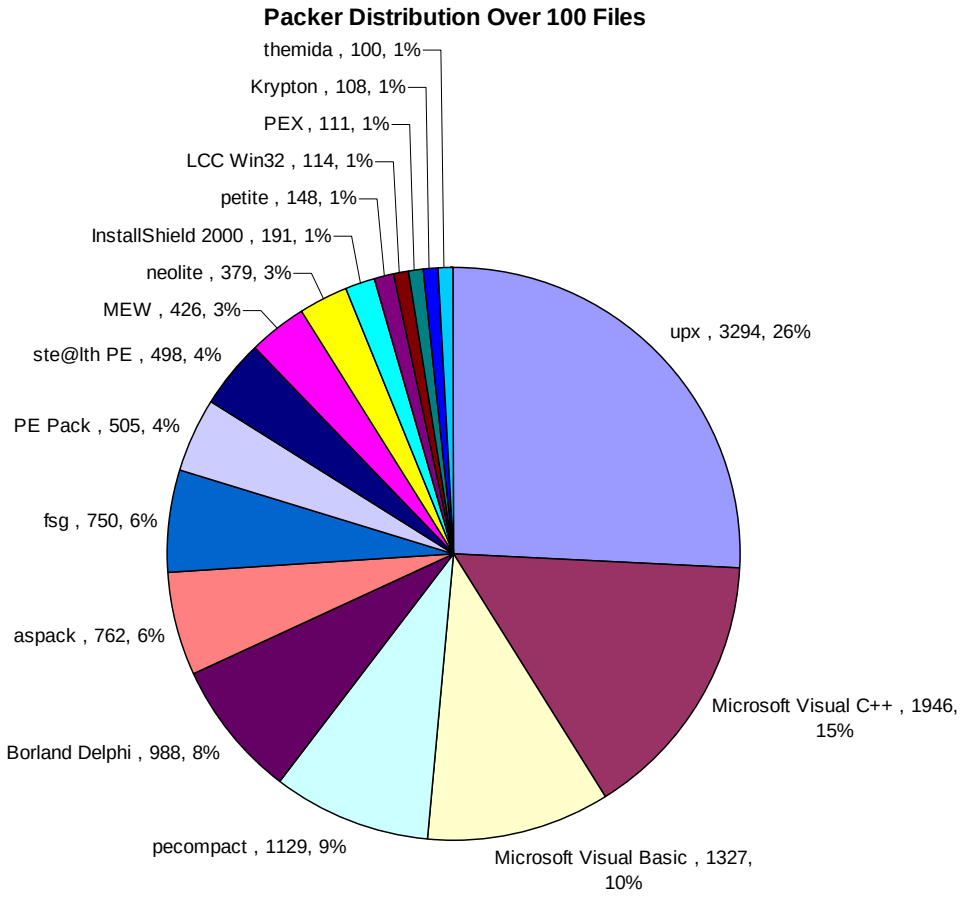
Packers

- Out of *31996* samples *37.9%* had detected packers
- Our packer detection also tries to detect compiler
- Top five detected packers:
  - UPX
  - PECOMPACT
  - ASPACK
  - FSG
  - PE PACK

Packers

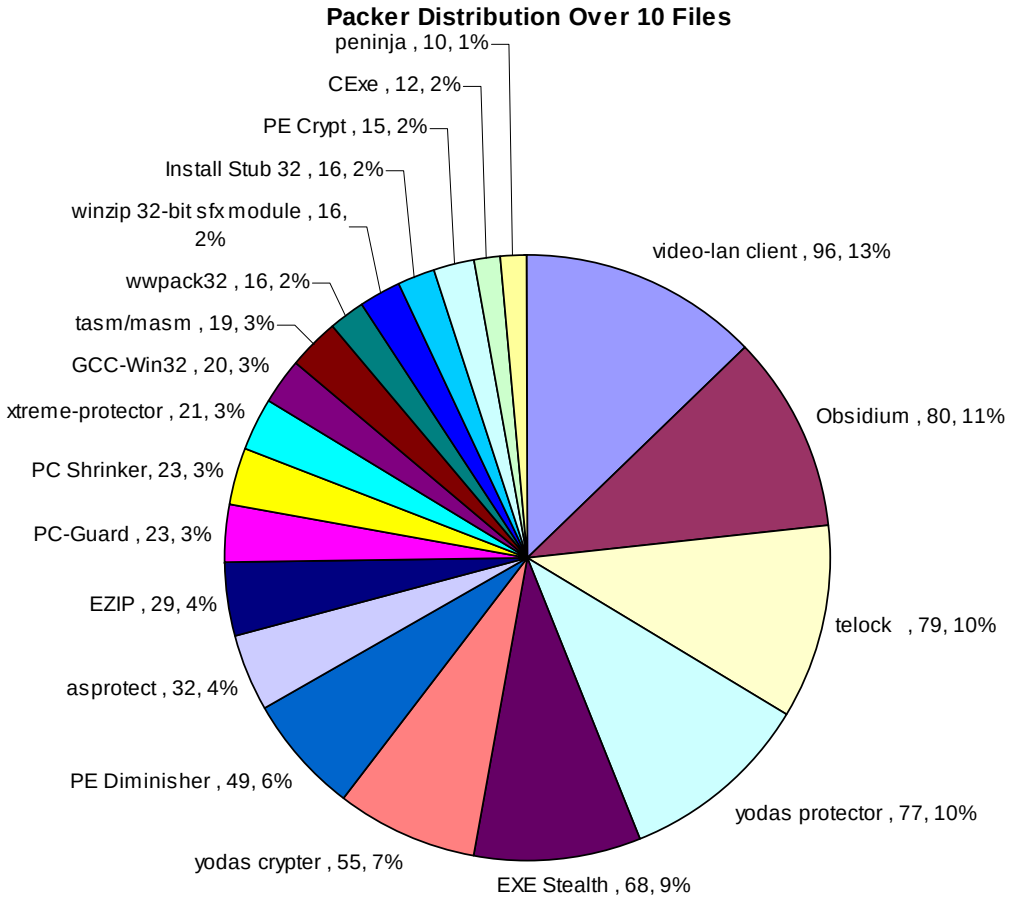
- Compilers detected in order:
  - Microsoft Visual C++
  - Microsoft Visual Basic
  - Borland Delphi
- What's statistically significant?
  - Most used packers
  - But also least used packers

Packers



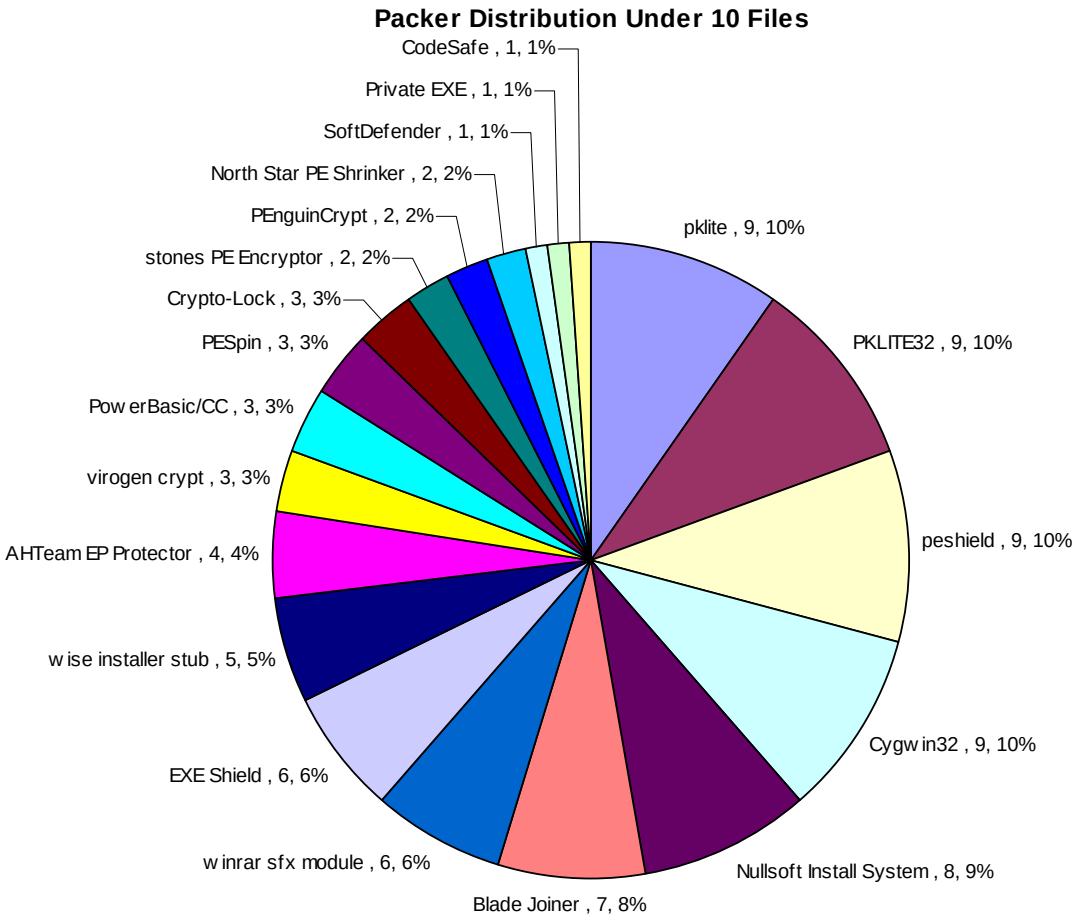
More than 100 files detected with packer listed

Packers



More than 10 files but less than 100 detected with packer listed

Packers



Less than 10 files detected with packer listed

Anti-virus

Detection statistics

Don’t base purchasing decisions on these figures!
Rough / inaccurate numbers!

Out of 31996 samples tested, each AV detected:

BitDefender	29127	91.0%
AVG	28095	87.8%
F-Secure	27972	87.4%
Kaspersky	27979	87.4%
Avast	27777	86.8%
McAfee	27061	84.5%
Antivir	26388	82.4%
ClamAV	24496	76.5%
F-Prot	24048	75.1%

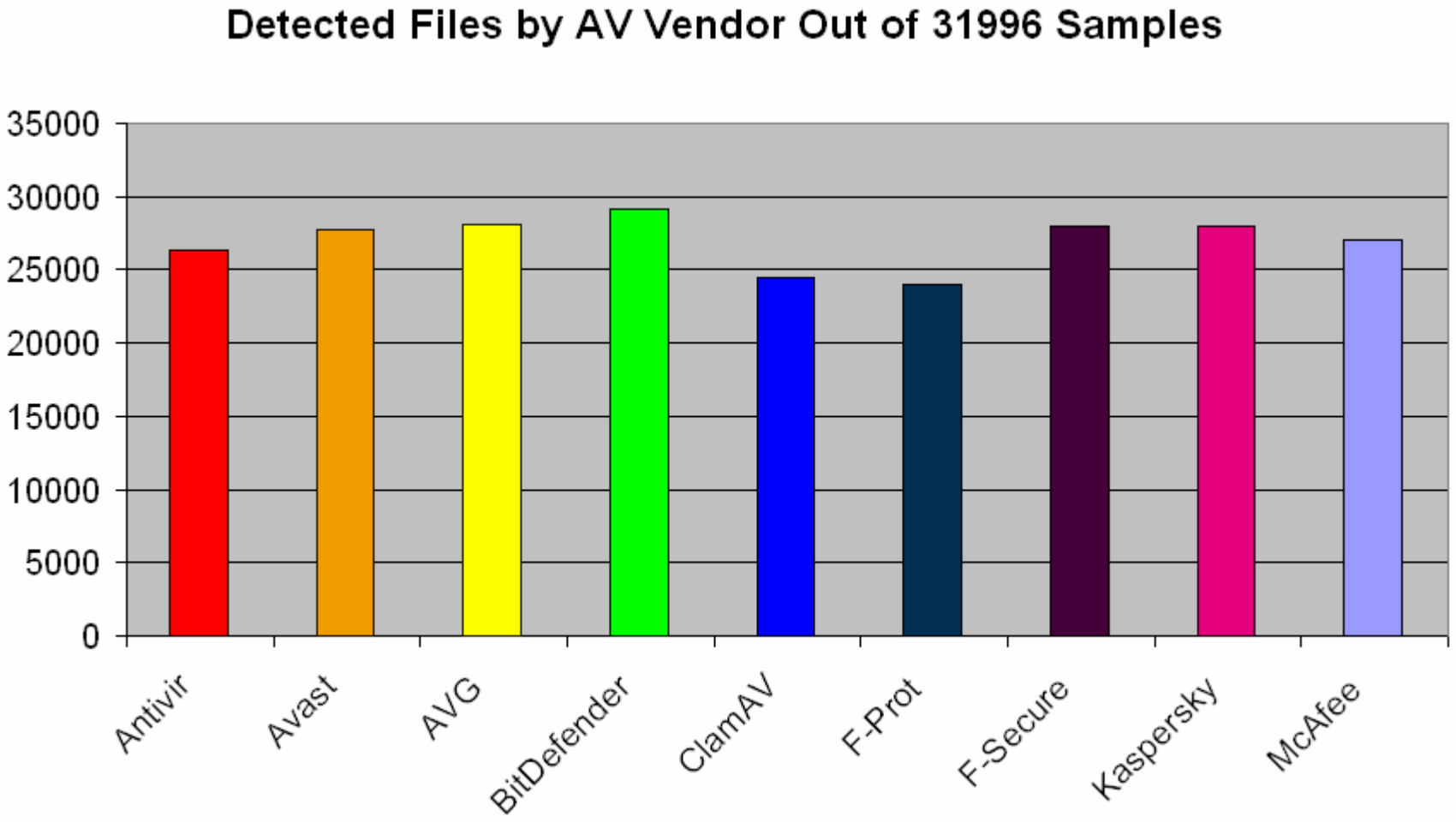
Anti-virus

Detection statistics

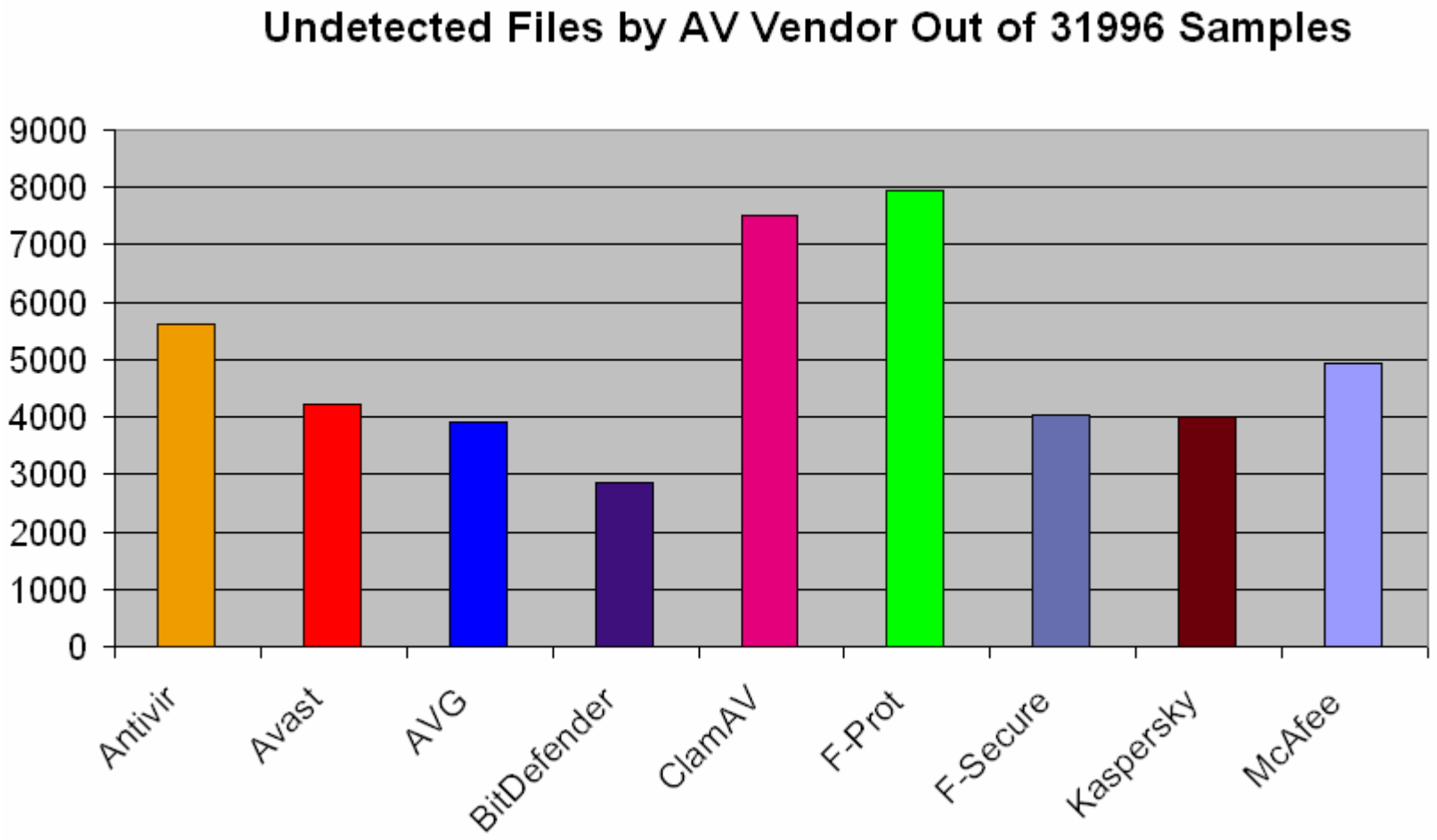
- 446 files not detected by any AV (could be non-malware)
  - The few of these manually tested were malicious
- Out of 31996 samples tested, each AV failed to detect:
  - Range of 5079 between worst and best

Antivir	5608	17.5%
Avast	4219	13.1%
AVG	3901	12.1%
BitDefender	2869	8.0%
ClamAV	7500	23.4%
F-Prot	7948	24.8%
F-Secure	4024	12.5%
Kaspersky	4017	12.5%
McAfee	4935	15.4%

Anti-virus


Detected Files by AV Vendor Out of 31996 Samples
35000
30000
25000
20000
15000
10000
5000
0
Antivir
Avast
AVG
BitDefender
ClamAV
F-Prot
F-Secure
Kaspersky
McAfee

Anti-virus


Undetected Files by AV Vendor Out of 31996 Samples
9000
8000
7000
6000
5000
4000
3000
2000
1000
0
Antivir
Avast
AVG
BitDefender
ClamAV
F-Prot
F-Secure
Kaspersky
McAfee

What else can we find

- Collecting the strings from each binary
  - Packed bins still often have info
- Strings give us clues into malware trends
- Financial related strings growing
- E-mail addrs, URLS, IP’s etc. useful for finding call home connections
- Trends?

URLS

- Parsing the malware strings yields interesting results
- 123 Russian URLS
  - http://catalog.zelnet.ru/
  - http://binn.ru/
  - http://www.aktor.ru/
  - http://av2026.comex.ru/
  - http://www.free-time.ru/
  - http://momentum.ru/
  - http://www.elemental.ru/
  - http://mir-vesov.ru/p/lang/CVS/
  - http://www.scli.ru/
  - http://sacred.ru/
  - http://pocono.ru/

URLS

- URLs with the word “hack”:
  - Http://www.Geocities.com/Hack_A_Freind_inc/
  - http://1337suxx0r.ath.cx:580/hack/sneaker/
  - http://www.hack-info.de/
  - http://www.hacknix.com/~rnsys/
  - http://hackzzz.narod.ru/
  - http://www.micro-hack.com/
  - http://www.outergroup.com/hacktack/
  - http://www.hack-gegen-rechts.com/
  - http://www.immortal-hackers.com/
  - http://data.forumhoster.com/forum_hackersnet/
  - http://www.shadowhackers.de.vu/
- (These are the SMART hackers :)

URLS

- Government sites referenced:
  - HTTP://WWW.CAIXA.GOV.BR/
  - http://camaramafra.sc.gov.br/1/
  - http://www.receita.fazenda.gov.br/
  - http://www.lfxmsc.gov.cn/
  - http://hbh.gov.cn/inc/
  - http://hbh.gov.cn/gg/
  - http://shadowvx.gov/benny/viruses/

URLS

- 39 IP addresses (call back / C&C?)
- 7 Chinese sites
- 3 Israeli sites
- 23 Brazilian (banker trojans?)
- 98 German urls
- 4 Romanian
- 9 Japanese
- vx.netlux.org/ shows up quite a bit

E-Mail addresses

- Only 67 total emails extracted
- 2 Russian Emails show up repeatedly
  - ltv@microset.ru
  - miklin@diakom.ru
- Xfocus guys probably from ripped exploit code
  - lashsky@xfocus.org
  - benjurry@xfocus.org

Interesting Strings

- Lots of useful words found in malware
- The word “BANK” shows up x times
- “CREDIT” shows up x times
- “SOCIAL SECURITY” / “SSN” show up x times
- Owned x times
- Hack x times
- Deface x times

Interesting Strings

- $remote_addr="http://127.0.0.1/~snagnever/defacement/paginanova/";//url

Interesting Strings

- Yo momma so old her social security number is 1!

Interesting Strings

- CCALG - Credit Card Generator.exe

Interesting Strings

- Enter credit card number here to verify

Interesting Strings

- [TFTP]: I just owned: %s (%s).

Interesting Strings

- C:\[Rx-oWneD]_[Coded_NAPSTER_For_0lab-Team]\[Rx-oWneD] [Coded NAPSTER For 0lab-Team]\Debug\rBot.pdb

Interesting Strings

- HI HackeR, HenKy LiveS HerEf

Interesting Strings

- Only a Joke!!!!!! JOKE The Web station has been HACKED Ha Ha Ha!!.

Interesting Strings

- Citibank Australia
- Wachovia Online Business Banking
- Unibanco
- Bank of America

Conclusion

- Large collection of malware provides data mining opportunity
- Not best way to test AV but interesting results
- Why don’t malware authors use tougher packers more often?
- Financial attacks prevalent (we already knew that)

Questions ?

- Thanks to *krbkelpto*, *Danny Quist*, Metasploit, #vax and the rest of OCDEV team!
- Thank you!