Mince Research

Bypassing Corporate Email Filtering

Simon Howard
Ruxcon 2006

Introduction

"Emails were sent to specific individuals within the organization that contained a Microsoft Word attachment. This attachment, when opened, exploited a previously-unknown vulnerability in Microsoft Word (verified against a fully-patched system).“

"It was addressed by name to the intended victim and not detected by the anti-virus software.“

http://isc.sans.org/diary.php?storyid=1345 [2006-05-19]

whoami

- Name: Simon Howard

- Occupation: Security engineer for DMZGlobal LTD
  - Firewalls
  - Routing / Switching
  - Hosting
  - Email / Web
  - Consultancy

- First Computer: ZX81

Presentation Overview

Service Discovery
- smtpscan
- Message Headers
- File Association

Antivirus
- Engine Capabilities
- Product Determination
- Unscannable Files

Content Filtering
- Extension Stripping
- Content-Type Trickery
- File Type Checking
- Message Splintering

Mitigation at each stage

Presentation Overview

Bypass Through Compromise
- pirana

Email Test Suite
- Example usage
- eicar.com collection

Conclusion & Questions

Attacker Motives

Email is still business critical for the majority of organisations

Compromise gateway
- Intercept all communications
- Use machine as open relay

Desktop Infection
- Addition of host to botnet
- Obtain commercial secrets from competitors
- Collect all doc, pdf, xls, autocad files

Service Discovery

- smtpscan
- Message Headers
- File Association
- Mitigation

smtpscan

```
$smtpscan 192.168.0.1
  15 tests available
  3185 fingerprints in the database

Scanning 192.168.0.1 port 25
 15/15

Result --
250:501:501:250:553:553:550:214:252:502:502:502:…

Banner :
220  ESMTP    This is a private system, bugger off.

SMTP server corresponding :
  - Sendmail 8.12.2-8.12.5
  (with source email address checking like RBL)
```

HELP & VERSION

- Use p0f to enumerate underlying OS

- Sometimes a simple HELP command is all that's needed

```
Connected to 192.168.0.1.
Escape character is '^]'.
220  ESMTP This is a private system, bugger off.
help
214-2.0.0 This is sendmail version 8.11.7p2+Sun
```

- VERSION / HELP VERSION are also useful

```
HELP VERSION
214-Receiver Version 5.5.6.7 (5.5.6.0)
214-Engine Version 5.5.6.7 (5.5.6.0)
214-Sender Version 5.5.6.7 (5.5.6.0)
214 Controller Version 5.5.6.7 (5.5.6.0)
```

X-MimeOLE

Microsoft Exchange information

```
X-MimeOLE: Produced By Microsoft MimeOLE V5.00.2615.200
X-MimeOLE: Produced By Microsoft Exchange V6.0.5762.3
X-MimeOLE: Produced By Microsoft Exchange V6.5.6944.
```

Message-ID's often contain interesting information

```
Message-ID: <6489015.99029557.JavaMail.nobody@example.org>
```

So do Received headers

```
Received: from [192.168.0.1] (helo=yfoikf.tzsvt) by
 192.168.0.2 with smtp (Exim 4.43) id 1FcAp8-xx1af-91; Sat,
 6 May 2006 02:39:06 +0200
```

Backup MX'es

Tertiary MX anyone?

```
;; ANSWER SECTION:

mince.govt.nz.     193     IN      MX      10 gate1.mince.govt.nz.
mince.govt.nz.     193     IN      MX      15 gate2.mince.govt.nz.
mince.govt.nz.     193     IN      MX      30 mx.clear.net.nz.
```

File Association

Attachment Types

- How many file types are natively executable?
- Default Windows file associations (cab, zip, cpl, vbs)

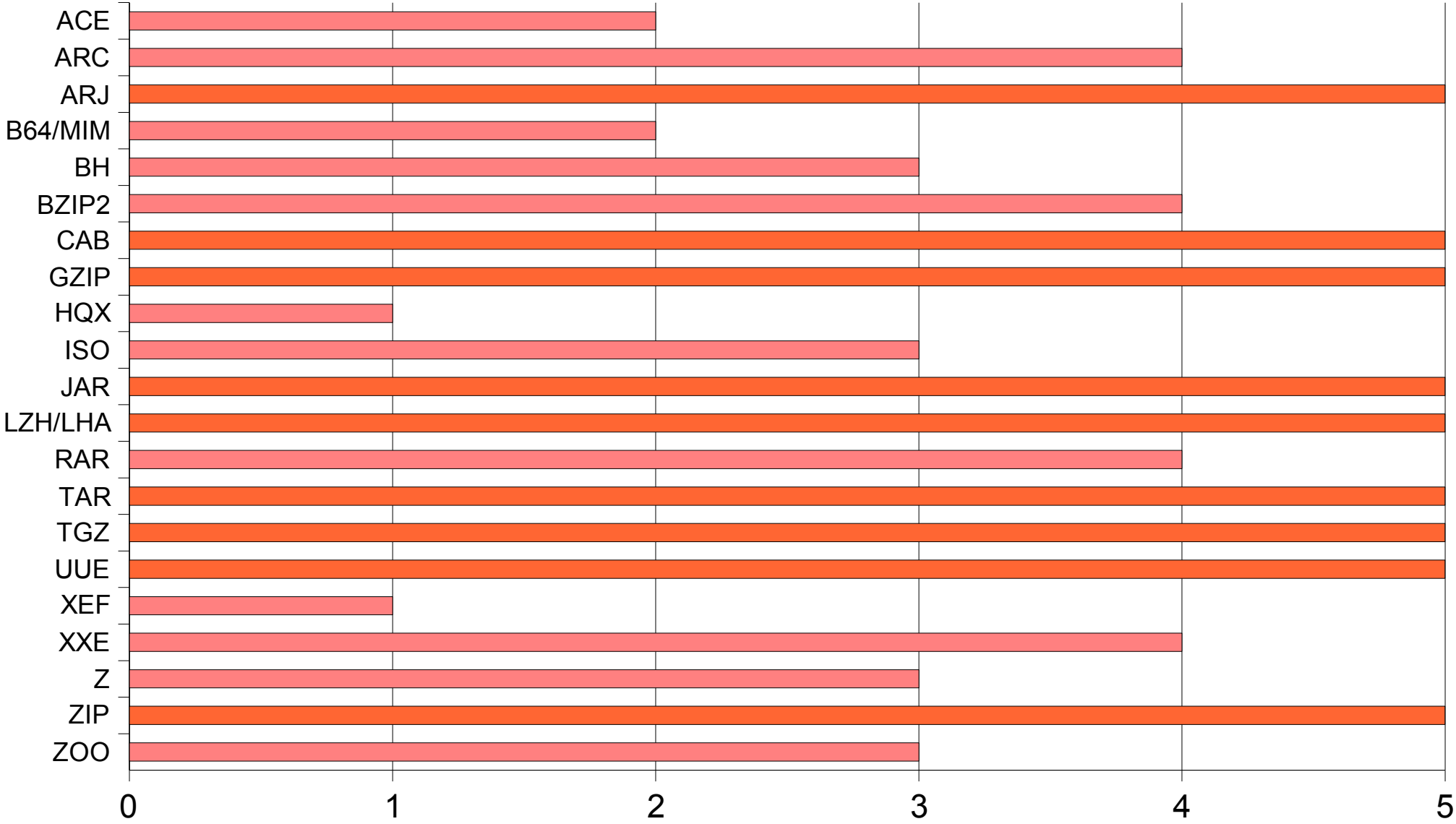
What about supported compression algorithms…

- CD writing software (iso, cue, bin)
- Desktop decompression software
- WinZip / WinRar / WinAce / Power Archiver / PicoZip

```
eicar.arj:  ARJ archive data, v11, slash-switched, os: Unix
```

Decompression Software

Desktop Decompression Software vs Supported Algorithms



Service Discovery Mitigation

Good Ideas:

- Remove all valuable information from SMTP gateway

- LDAP - Client MTA will generate bounce messages

```
mail from: user@test.net
250 2.5.0 Address Ok.
rcpt to: nosuchusr@example.org
550 5.2.1 User unknown: nosuchusr@example.org
```

- Remove / Replace “Received: from” headers

- Remove “X-MimeOLE” headers

- Disable unneeded file associations

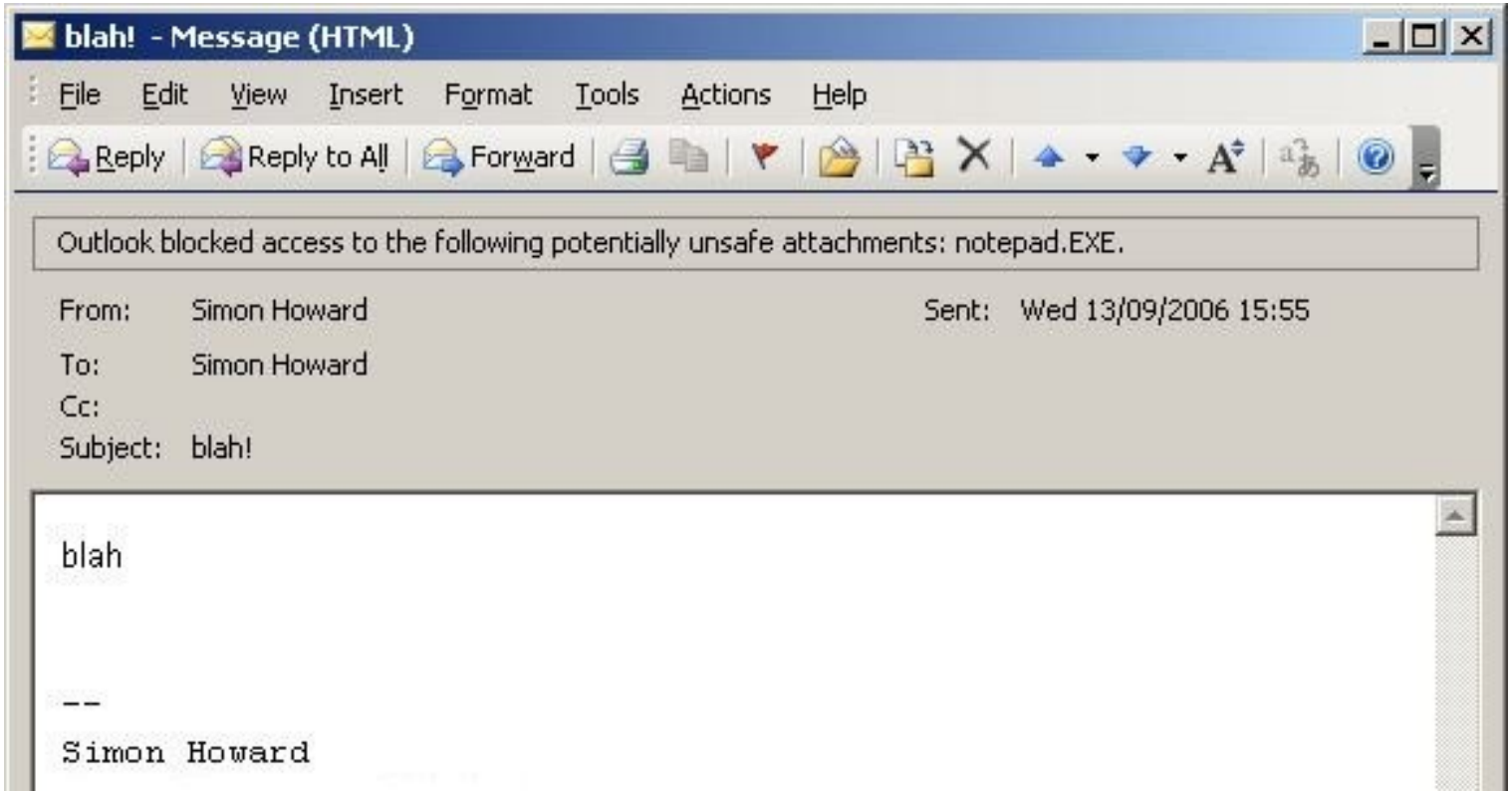
- Patch!

Service Discovery Mitigation

Good Ideas:

- Disable HELP / HELP VERSION

- Block dangerous attachments at the Exchange level



Service Discovery Mitigation

Not so good ideas:

- Disable bounce messages

- Modify error / success codes

Antivirus

- Engine Capabilities
- Product Determination
- Unscannable Files
- Mitigation

Antivirus Software

Antivirus software varies greatly in:

- Quality
- Policy features
- Decompression algorithm support
- Executable unpacker support
- Heuristic abilities

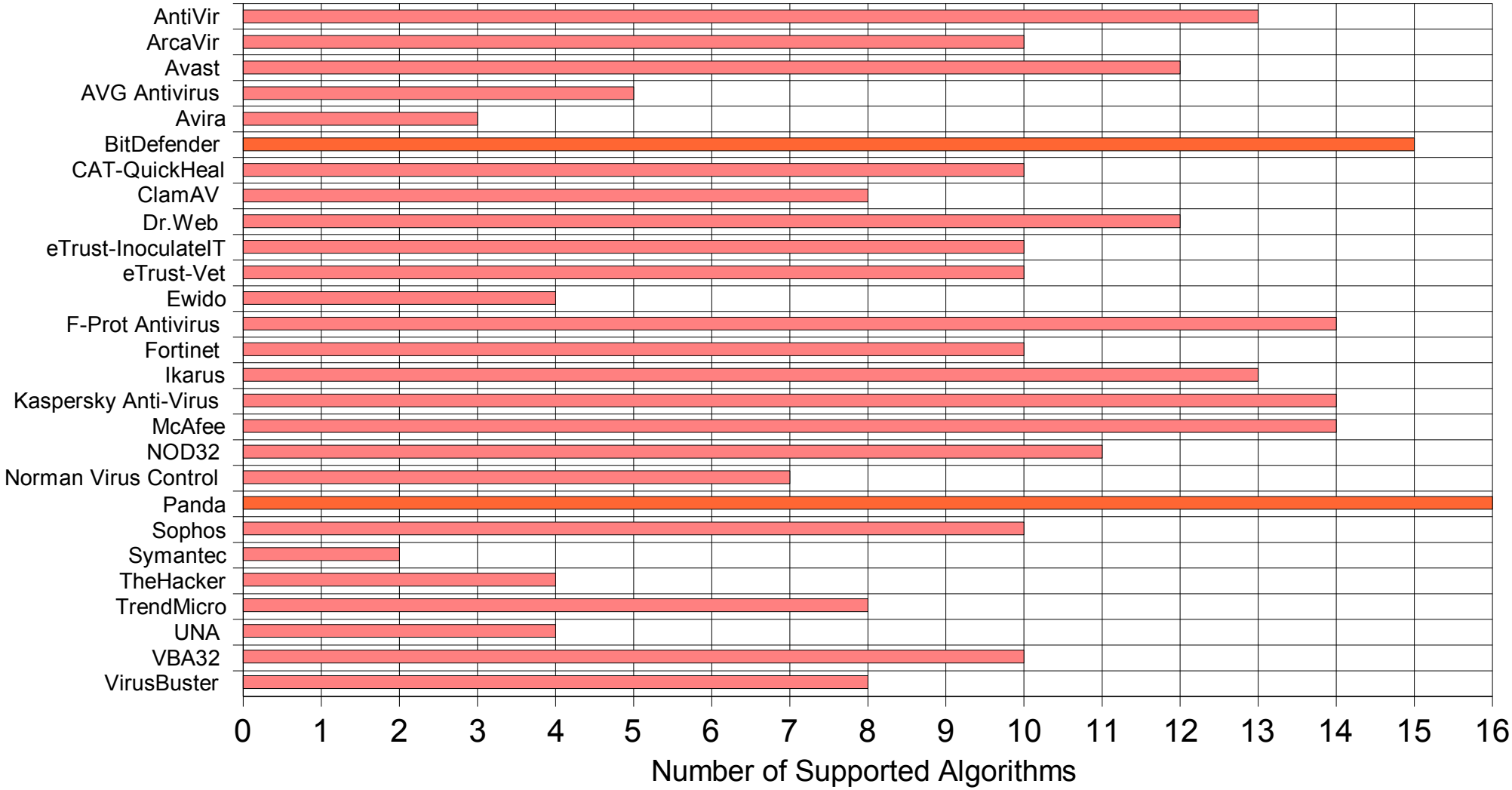
eicar.com

68 byte file used to verify that your antivirus software is operating correctly.

```
eicar.arc:      ARC archive data, uncompressed
eicar.bh:       data
eicar.arj:      ARJ archive data, v11, slash-switched, os: Unix
eicar.b64:      ASCII text
eicar.cab:      Microsoft Cabinet file, 146 bytes, 1 file
eicar.com:      ASCII text, with no line terminators
eicar.bz2:      bzip2 compressed data, block size = 900k
eicar.gz:       gzip compressed data, was "eicar.com", from Unix
eicar.hqx:      BinHex binary text, version 4.0
eicar.iso:      ISO 9660 CD-ROM filesystem data 'CDROM '
eicar.jar:      Zip archive data, at least v2.0 to extract
eicar.lha:      LHarc 1.x archive data [lh0]
eicar.lzo:      lzop compressed data - version 1.020, os: Unix
eicar.rar:      RAR archive data, v1d, os: Unix
eicar.tar:      POSIX tar archive
eicar.uue:      uuencoded or xxencoded text
eicar.zip:      Zip archive data, at least v1.0 to extract
eicar.zoo:      Zoo archive data, v2.10, modify:v2.0+, extract:v1.0+
```

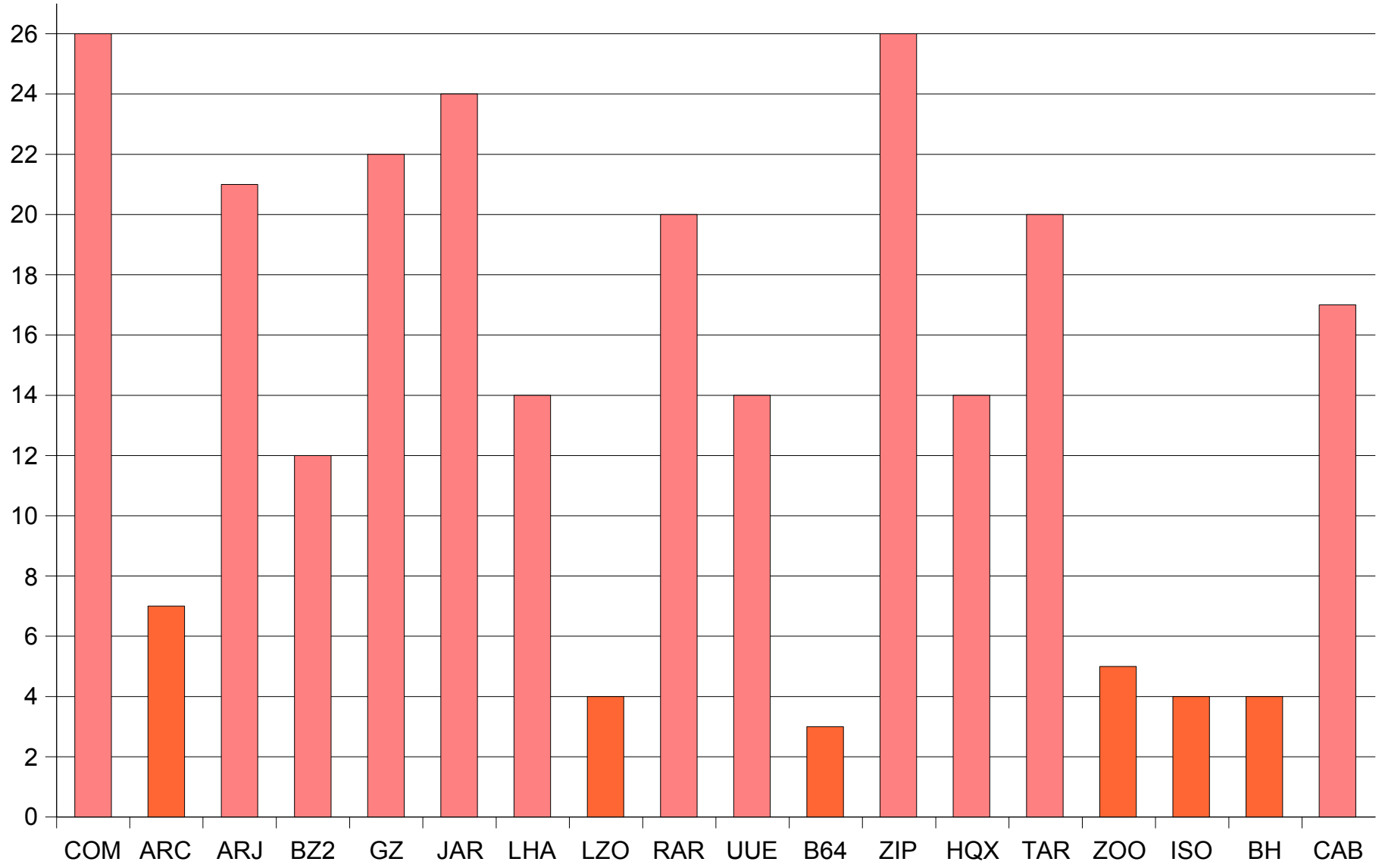
Vendor vs Compression

Antivirus Vendor vs Supported Compression Algorithms



Algorithm vs Vendor

Compression Algorithm Type vs Antivirus Vendor Support



Product Determination

Determine antivirus software used:

- smtpscan

- Capture bounce messages

1. Send compressed files to target containing eicar.com
2. If bounce message returned, algorithm not supported
3. Product used can be guessed using Matrix

- Market coverage

1. Compression supported by the majority of desktop applications
2. Decompression unsupported by the majority of AV vendors

Unscannable/Encrypted Files

Sophos example

Scannable:
(21 NotAMonth 2001 3:15pm) Tj

UnScannable:
(21 August 2006 3:15pm) Tj

Password protected archive
- image containing password

Encryption

Scanning Boundaries

Multiple layers of compression
- Same compression algorithm (zip->zip->zip)
- Multiple compression algorithms (zip->tar->zoo)

Multiple files in the same archive
- 10,000 files (Recycled folder)

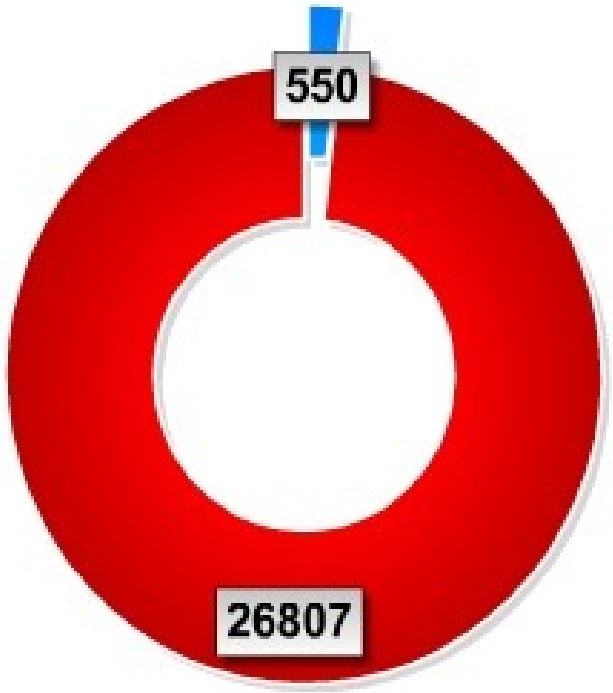
Compression ratio
- zip bombs (DoS)

Large files

Failure to Detect

No need to worry about the AV software really, it's not going to detect much...

Failures in Detection (Last 7 Days)



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

13:53 09/12/2006 CEST

http://www.virustotal.com/vt/en/estadisticasf?detection_failures

Antivirus Mitigation

- Use “best of breed” products at the gateway

- Implement Heuristic / VM engines (Norman Sandbox)

- Utilise a different AV product on the desktop

- Add support for more decompression algorithms

- Set sensible limits on compressed files

- Quarantine Encrypted / Unscannable files

- Upgrade Antivirus Engines / Patterns regularly

- Patch!

Content Filtering

- Extension Stripping
- Content-Type Trickery
- File Type Checking
- Message Splintering
- Mitigation

Extension Stripping

Something along the lines of *.exe or (?i)\.exe$

RFC-2047 allows quoted-printable and base64

```
filename=?us-ascii?Q?<string>?="
filename=?us-ascii?B?<string>?="
```

Double encode?
- base64 + quoted-printable

Tried various combinations against multiple products
- vendor patching in progress :)

UUEncode

```
begin 644 eicar.com
M6#5/(5`E0$%06S1<4%I8-30H4%XI-T-#*3=])$5)0T%2+5-
404Y$05)$+4%.
75$E625)54RU415-4+49)3$4A)$@K2"H`
`
end
```

- OR

```
begin-base64 644 eicar.com
WDVPIVAlQEFQWzRcUFpYNTQoUF4pN0NDKTd9JEVJQ0FSLVNUQU5EQVJE
LUFO
VElWSVJVUy1URVNULUZJTEUhJEgrSCo=
====
```

Content-Type Checking

```
Content-Disposition: attachment; filename="file.xls"
Content-Transfer-Encoding: base64
Content-Type: application/ms-word; name="file.xls"
```

- Easy to modify

```
./ets.pl -a file.xls -at application/ms-meat
```

File Type Checking

Missing MIME boundary

```
Content-Transfer-Encoding: 7bit
Content-Type: multipart/mixed; boundary="_----------=_1158149887273900"
MIME-Version: 1.0
Date: Wed, 13 Sep 2006 12:18:07 UT
From: somebody@example.org
To: user@somewhere.com
Subject:eat my exe
X-Mailer: MIME::Lite 3.01 (F2.74; B3.07; Q3.07)

This is a multi-part message in MIME format.

--_----------=_1158149887273900
Content-Disposition: attachment; filename="test.exe"
Content-Transfer-Encoding: base64
Content-Type: application/ms-word; name="test.exe"

b25jZSB1cG9uIGEgdGltZQo=

<snip> --_----------=_1158149887273900-- </snip>
```

Message Splintering

Some of the less advanced products do not splinter messages properly

Policy 1: Recipient - bob@example.org
- No attachment stripping

Policy 2: Recipient - sam@example.org
- Strip all attachments

```
mail from: me@test.org
rcpt to: bob@example.org
rcpt to: sam@example.org
```

Content Filtering Mitigation

Attachment Stripping
- File Extension (case insensitive)
- Content-Type
- File Type (add additional file types)

Message Splintering
- default_destination_recipient_limit = 1

Convert Microsoft document formats to plain-text / CSV

Watermark important documents
- Check for this fingerprint on all outbound emails

Implement inbound & outbound filtering
- Stops you from infecting the rest of the world

Bypass Through Compromise

If a vulnerability is found in RAR, chances are the AV vendors have used the same libraries to support decompression for RAR in their product.

Keep an eye on the advisories after a major flaw is found in a common decompression library. Watch all the AV vendors rush to (silently) patch their products

Pirana [sic]

Coded by Jean-Sébastien Guay-Leroux

- Penetration testing framework for SMTP content filtering

- Join several attachments with various offsets in a single email

- The content filter will analyse each attachment in turn but only register it as one message

Invisible picture

```
<img src="cid:file-01" height=0 width=0>
```

multipart/alternative

- HTML + plain-text version version are both present in the same email
- Define attachments as multipart/alternative, if HTML version of the message exists, the attachments will be invisible and the HTML rendered

Pirana Supported Overflows

Integrated with metasploit (bit dirty)

```
$ ./pirana.pl -h
Usage: pirana.pl [MANDATORY ARGS] [OPTIONAL ARGS]

Valid exploits numbers:
  0 OSVDB #5753:  LHA get_header File Name Overflow
  1 OSVDB #5754:  LHA get_header Directory Name Overflow
  2 OSVDB #6456:  file readelf.c tryelf() ELF Header Overflow
  3 OSVDB #11695: unarj Filename Handling Overflow
  4 OSVDB #23460: ZOO combine File and Dir name overflow
```

Fuzz your own!

Email Test Suite

ets.pl

- charset

- transfer-encoding

- content-type

- content-type name

- add attachments

- compress attachments

- output raw message to stdout

ETS - Content-*

```
$ ./ets.pl -ae help

  Supported Content-Transfer-Encodings are defined in RFC-2045:
    7bit - guarantees no 8 bit chars, lines do not exceed 1000 chars
    8bit - might contain 8 bit chars, lines do not exceed 1000 chars
    base64 - used to encode arbitrary octet sequences
    binary - might contain 8 bit chars, lines may exceed 1000 chars
    quoted-printable - useful for encoding non-ASCII charaters

$ ./ets.pl -at help

  Supported Content-Types are defined in RFC-2046:
    For example:
     application - application/octet-stream, application/gzip
     audio       - audio/basic
     image       - image/gif, image/jpeg
     message     - message/rfc822
     multipart   - multipart/mixed, multipart/alternative
     text        - text/plain, text/html
     video       - video/mpeg
```

ETS – Compression

```
$ ./ets.pl -z help

arc:     Supported   -> /usr/bin/arc
arj:     Supported   -> /usr/bin/arj
b64:     Supported   -> /usr/bin/uuencode
bz2:     Supported   -> /bin/bzip2
gz:      Supported   -> /bin/gzip
hqx:     Supported   -> /opt/stuffit/bin/stuff
iso:     Supported   -> /usr/bin/mkisofs
jar:     Supported   -> /usr/bin/jar
lha:     Supported   -> /usr/bin/lha
lzo:     Supported   -> /usr/bin/lzop
rar:     Supported   -> /opt/bin/rar
shar:    Supported   -> /usr/bin/shar
tar:     Supported   -> /usr/bin/tar
uue:     Supported   -> /usr/bin/uuencode
zip:     Supported   -> /usr/bin/zip
zoo:     Supported   -> /usr/bin/zoo
```

ETS - Example

```
./ets.pl -f test@example.org \
         -t test@test.com \
         -d 192.168.0.1 \
         -s test \
         -a test.xls \
         -ae binary \
         -at application/ms-meat \
         -z zoo \
         -zo test.zoo \
         -p stdout
```

ETS - Output

```
Content-Transfer-Encoding: 7bit
Content-Type: multipart/mixed; boundary="_----------=_1158580521214960"
MIME-Version: 1.0
Date: Mon, 18 Sep 2006 11:55:21 UT
From: test@example.org
To: test@test.com
Subject: test
X-Mailer: MIME::Lite 3.01 (F2.74; B3.07; Q3.07)

This is a multi-part message in MIME format.

--_----------=_1158580521214960
Content-Disposition: inline
Content-Length: 23
Content-Transfer-Encoding: binary
Content-Type: text/plain

this is the message body

--_----------=_1158580521214960
Content-Disposition: attachment; filename="test.zoo"
Content-Length: 169
Content-Transfer-Encoding: binary
Content-Type: application/ms-meat; name="test.zoo"

ZOO 2.10 Archive.    *    *    qq25  test.xls
 HE @@)#(
--_----------=_1158580521214960--
```

eicar.com collection

The eicar.com collection

http://research.mince.ac.nz/eicar-collection.zip
- might trigger your antivirus software :)

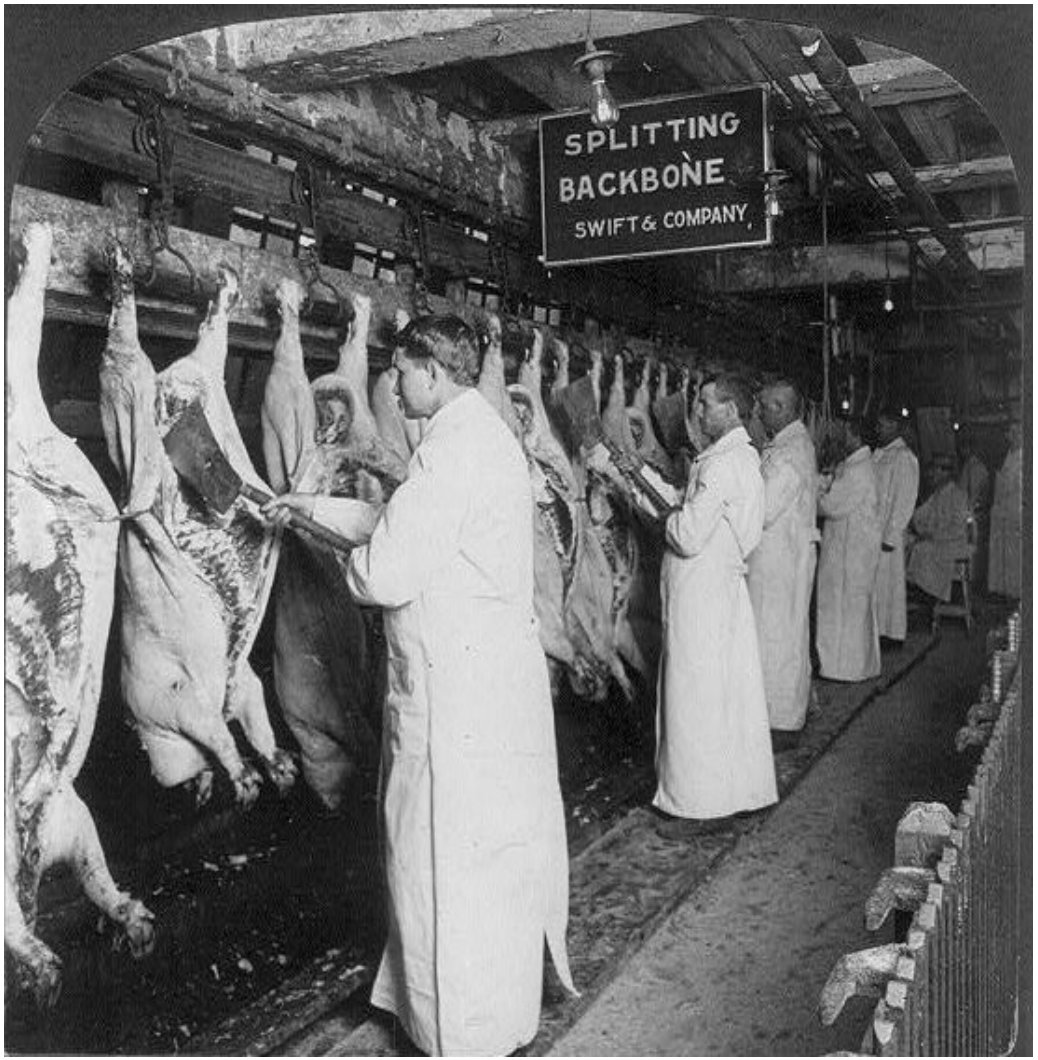
Conclusion

Pattern-based antivirus software is glue and duct-tape for an end of life technology

Thoroughly evaluate content filtering and antivirus software before purchasing

Thoroughly test your own email gateways capabilities

Questions?



http://research.mince.ac.nz
si@mince.ac.nz

References

Bypassing content filtering whitepaper - 3APA3A
http://www.security.nnov.ru/advisories/content.asp

Jotti's malware scan
http://virusscan.jotti.org/

Eicar anti-virus test file
http://www.eicar.com/anti_virus_test_file.htm

header_checks(5)
http://www.postfix.org/header_checks.5.html

pirana
http://www.guay-leroux.com/projects.html

p0f
http://lcamtuf.coredump.cx/p0f.shtml

smtpscan
http://www.greyhats.org/?smtpscan

Standard for the Format of ARPA Internet Text Messages
http://www.faqs.org/rfcs/rfc822.html

Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies
http://www.faqs.org/rfcs/rfc2045.html

Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types
http://www.faqs.org/rfcs/rfc2046.html

Multipurpose Internet Mail Extensions (MIME) Part Three: Message Header Extensions for Non-ASCII Text
http://www.faqs.org/rfcs/rfc2047.html

wvWare
http://wvware.sourceforge.net/

Virustotal
http://www.virustotal.com/