genua Ein Unternehmen der Bundesdruckerei

Umgehung von Firewalls auf Applikationsebene

Steffen Ullrich, genua GmbH

15. Deutscher IT-Sicherheitskongress

17.Mai 2015

Inhalt des Vortrags

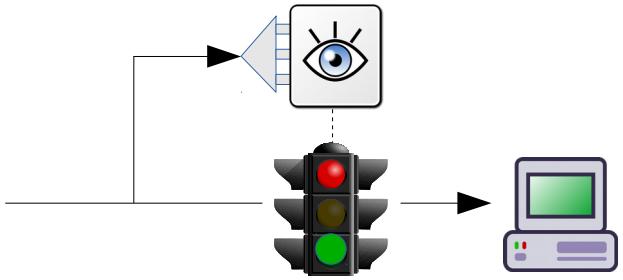
genua Ein Unternehmen der Bundesdruckerei

- Angriffe gegen Endanwender heutzutage primär über Web und Mail
- klassische Paketfilter wie iptables bieten hier keinen Schutz
- diverse Technologien und Buzzwords versprechen Analyse auf Applikationsebene: DPI, ALG, IDS, IPS, SG, NGFW, UTM, ...
- **Umgehung Analyse oft trivial möglich: Wie, Warum, Wie geht es besser**

genua Ein Unternehmen der Bundesdruckerei

- Steffen Ullrich
- seit 2001 bei genua GmbH
  - maßgeblich beteiligt an Entwicklung High Resistance Firewall genugate
- vorgestellte Ergebnisse sind Nebenergebnis aus Forschungsprojekten
  - Padiofire (2011-2013):
    Absicherung Web 2.0 in Perimeterfirewall
  - APT-Sweeper (2014-...):
    Neue Techniken gegen gezielte Angriffe
  - gefördert vom BMBF

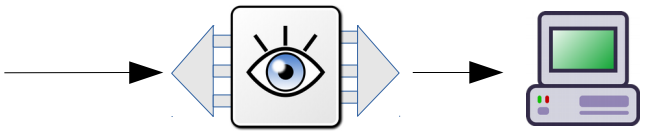
genua Ein Unternehmen der Bundesdruckerei



Passive Analyse

Entpacken
+ Analyse
+ Pass|Block

Blockieren oder Durchlassen der originalen Daten



Aktive Analyse

Entpacken
+ Analyse
+ Verpacken

Blockieren oder Weiterleiten der evtl. modifizierten Daten

Aktive Analyse bietet mehr Sicherheit als passive Analyse

```
GET / HTTP/1.1
Host: www.example.com
Accept-Encoding: gzip, deflate
```

Auswahl der Kompressionsmethode erfolgt basierend auf dem, was Client anbietet.

```
HTTP/1.1 200 ok
Content-Encoding: gzip
Content-length: 200
```

200 Bytes mit gzip komprimierte Daten

Weitere Methoden: sdch, br, lzma, ...

- brotli(br) ist neue Kompressionsmethode
- seit 2016 in Firefox, Chrome und Opera
  demnächst auch in Edge
- wird aktiv genutzt, z.B. durch Dropbox
  kann basierend auf Accept-Encoding des Browsers entscheiden, wie es komprimiert
- **Unterstützung in Firewalls ist marginal**
  kann ein Problem sein, muss es aber nicht

genua Ein Unternehmen der Bundesdruckerei

Aktive Analyse

kann Methode aus Accept-Encoding entfernen

```
GET / HTTP/1.1
Accept-Encoding:
  gzip,deflate,br
...

HTTP/1.1 200 ok
Content-Encoding: gzip
...
```

Inhalt komprimiert mit gzip

Passive Analyse

entweder implementieren
oder blockieren (Overblocking)
oder durchlassen (Bypass)

```
GET / HTTP/1.1
Accept-Encoding:
  gzip,deflate,br
...

HTTP/1.1 200 ok
Content-Encoding: br
...
```

Inhalt komprimiert mit brotli

genua Ein Unternehmen der Bundesdruckerei

Line-Folding erlaubt Umbrechen langer Zeilen im HTTP-Header.
Feature ist sinnlos, weil es gibt keine Längenbegrenzung!
Clients interpretieren es daher unterschiedlich.

deflate
Firefox
Chrome
Opera
Safari

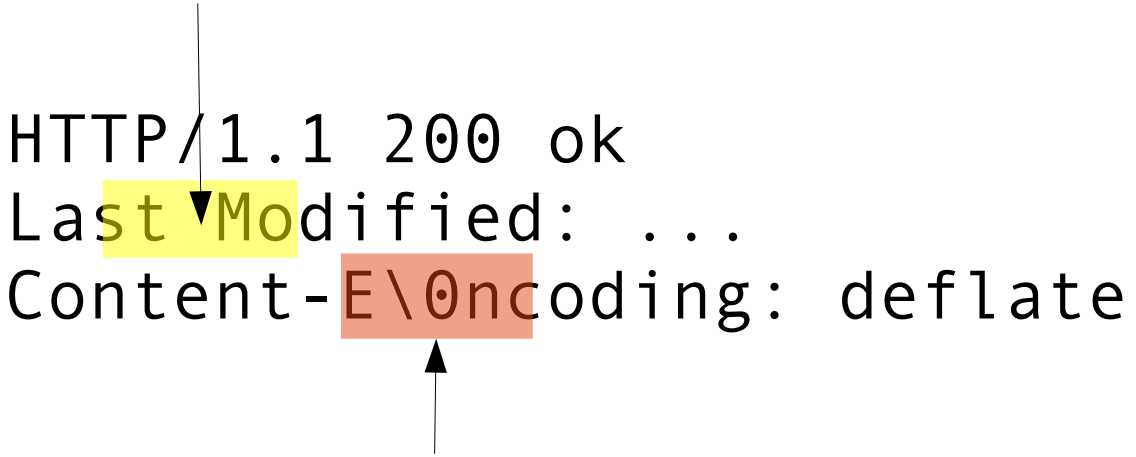
```
HTTP/1.1 200 ok\r\n
Content-Encoding:\r\n
<space>deflate\r\n
```

unkomprimiert
MSIE
MS Edge

Aktive Analyse
Bereinigen für einheitliche Interpretation

Passive Analyse
alle Varianten probieren
oder Blockieren (Overblocking)
oder Durchlassen (Bypass)

Leerzeichen im Key nicht erlaubt, kommt aber häufig vor.

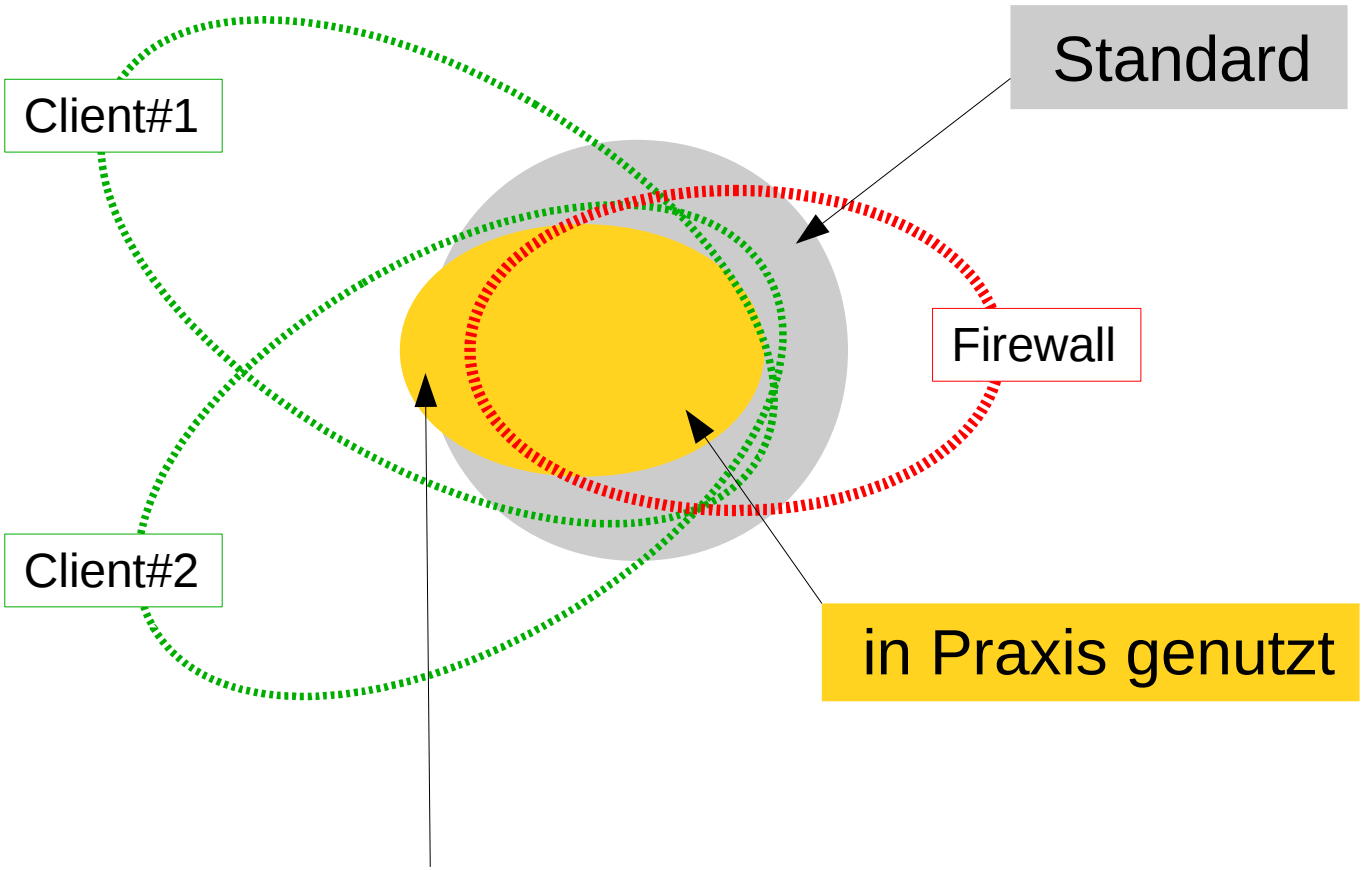


Ungültiges Zeichen \0 im Key.
Wird von Chrome ignoriert, d.h. sieht „Content-Encoding“ und interpretiert Body als komprimiert.

Aktive Analyse
klare Interpretation durch Bereinigen

Passive Analyse
Wieviel Kaputtheit darf bzw. muss man akzeptieren?

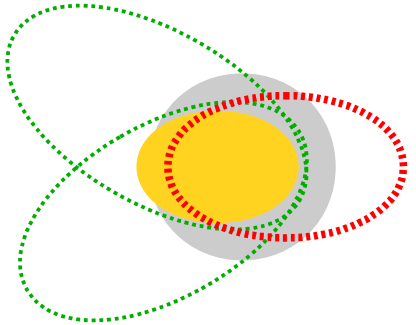
Interpretationslücke



Interpretationslücke

(Semantic Gap)

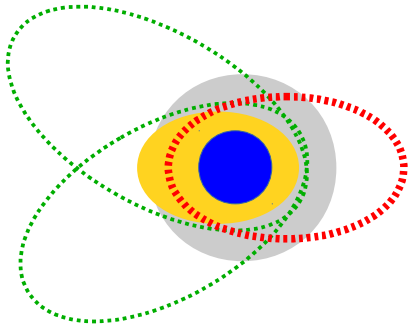
genua Ein Unternehmen der Bundesdruckerei



Kaputte Standards
unnötig flexibel und erweiterbar, human readable
widersprüchliche Aussagen möglich
keine sinnvolle Fehlerbehandlung festgelegt

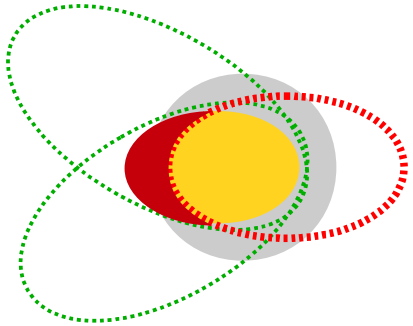
Kaputte Protokollparser
Einige Fehler im Protokoll werden teilweise explizit toleriert,
die meisten aber als Nebeneffekt der Implementation interpretiert.
Grundannahme ist, dass Gegenstelle protokollkonform arbeitet, d.h.
kaum explizite Fehlerbehandlung.

Fehlendes Bewusstsein in Firewalls
Angriffe auf dieser Ebene nicht erwartet.
Schlampige Parser, auf Geschwindigkeit statt Korrektheit getrimmt.



Aktive Analyse

Modifikation der Inhalte ermöglicht einheitliche Interpretation durch Reduktion auf **Kernprotokoll**.
Kann optionale Protokollfeatures aus Request entfernen.



Passive Analyse

Muss sämtliche Erweiterungen implementieren und sämtliche Varianten durchprobieren, sofern überhaupt bekannt.

Alternativen: Blockieren (Overblocking) bzw. Durchlassen (**Bypass**)

Jonathan Postel, RFC 761:

...follow a general principle of robustness:

be conservative in what you do,
be liberal in what you accept from others

Aktive Analyse

Kann modifizieren:
liberal what you accept
conservative what you do

Passive Analyse

Unveränderte Weiterleitung,
d.h. accept == what you do

liberal → Bypass
conservative → Overblocking

Aktiv vs. Passiv: Technologien, Produkte …

genua Ein Unternehmen der Bundesdruckerei

Passive Analyse	Aktive Analyse

DPI	ALG

IDS, IPS NGFW	Gateway, Proxy NGFW, UTM

Analysen sind unterschiedlich präzise implementiert, bedingt durch Performanceanforderungen, Kosten und Know-how.

Performance

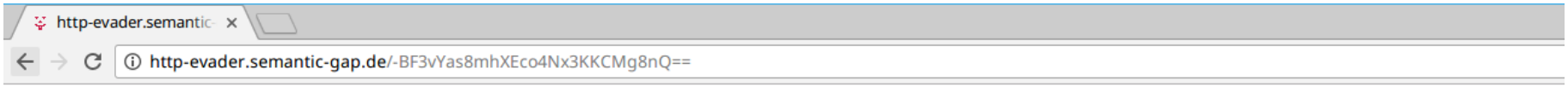
Erreichbare Sicherheit

genua Ein Unternehmen der Bundesdruckerei

- Testsystem zur Analyse des Verhaltens von Browsern und Firewalls
  - spezieller Webserver
  - automatische Durchführung von >750 Einzeltests im Webbrowser
  - Detektion von Bypass mittels EICAR-Testvirus
  - teilweise Detektion von Overblocking
  - Quellcode frei verfügbar
  - öffentliche Installation für schnelles Testen

HTTP-Evader im Bild

genua Ein Unternehmen der Bundesdruckerei



Firewall evasion test with EICAR test virus within eicar.zip

Progress: 38.3% - content-encoding deflate, first segment compressed with zlib but ADLER32 removed, next with deflate in new TCP packet

Serious Problems

[0] failure for valid response: junk before test virus TRY SRC
[0] failure for valid response: junk after test virus TRY SRC
[162] Evasion possible: content-encoding deflate, served with deflate TRY SRC
[163] Evasion possible: content-encoding deflate mixed case, served with deflate TRY SRC
[776] Evasion possible: "Content-encoding: <lots-of-spaces> deflate", served with deflate TRY SRC
[165] Evasion possible: content-encoding deflate, served with deflate with 2 compressed blocks with partial flush in between TRY SRC
[167] Evasion possible: content-encoding deflate, served with deflate with 2 compressed blocks with block flush in between TRY SRC
[169] Evasion possible: content-encoding deflate, served with deflate with 2 compressed blocks with sync flush in between TRY SRC
[171] Evasion possible: content-encoding deflate, served with deflate with 2 compressed blocks with full flush in between TRY SRC
[174] Evasion possible: content-encoding gzip, first segment compressed with gzip, next uncompressed TRY SRC
[176] Evasion possible: content-encoding deflate, first segment compressed with zlib, next uncompressed TRY SRC

Debug

[0] sanity check without test virus - match TRY SRC
[0] junk before test virus - change(200) TRY SRC
[0] junk after test virus - change(200) TRY SRC
[1] simple and valid chunking - change(200) TRY SRC
[1] simple and valid chunking - match TRY SRC
[2] content-length header, not chunked - change(200) TRY SRC
[2] content-length header, not chunked - match TRY SRC
[2] chunks size prefixed with 0 - change(200) TRY SRC

genua Ein Unternehmen der Bundesdruckerei

- Gartner Top UTM, Enterprise Firewalls, Cloud Security 2015 – Fail:
  - 85% deflate-Kompression
    von allen Browsern unterstützt, von vielen Firewalls nicht ausreichend
  - 70% manipulierte gzip-Kompression
    reservierte Bits gesetzt, falsche CRC, ... - siehe Tagungsband
  - 60% HTTP 0.9
    Protokoll seit 20 Jahren obsolet, aber implementiert in meisten Browsern
  - ...
- alle Firewalls betroffen in Q4/2015
- Situation jetzt etwas besser
  Aber selten 100% resistent bzw. nicht in Voreinstellung

genua Ein Unternehmen der Bundesdruckerei

- ursprünglich Mails nur ASCII
  mit höchstens 1000 Zeichen in Zeile
- MIME erlaubt innerhalb dieser Grenzen
  Attachments, auch binär
  Umlaute im Body, Header, Dateinamen
- mehrere RFC involviert
  sinnlos komplex, erweiterbar
  diverse unnötige Features
  teilweise unterspezifiziert
  teilweise widersprüchlich zu anderen Standards
  gefühlt schlimmer als HTTP
- **viele MUA und Tools erzeugen fehlerhafte Mails**

MIME – einführendes Beispiel

genua Ein Unternehmen der Bundesdruckerei

```
From: me@example.com
To: you@example.com
Subject: Viele =?UTF-8?Q?Gr=C3=BC=C3=9Fe?=
Content-type: multipart/mixed;
  boundary=trenner

--trenner
Content-type: text/plain; charset=UTF-8
Content-Transfer-Encoding: quoted-printable

Viele Gr=C3=BC=C3=9Fe von mir.
--trenner
Content-type: application/octet-stream;
  name=test.txt
Content-Disposition: attachment;
  filename*0*=utf-8''%c3%bcbel.e;
  filename*1=xe
Content-Transfer-Encoding: base64

TVqQ...VGhpcyBwcm9ncmFtIGNhbm5vdCBi...
--trenner--
```

Viele Grüße

Grüße

übel.exe

MZ...This program cannot be run in DOS mode...

RFC 2046
Unterteilung, Attachments
multipart/mixed
multipart/alternative, ...
Content-type: ...; name=

RFC 2045
binäre Inhalte → ASCII
base64, quoted-printable
Content-Type, Charset

RFC 2047
Umlaute etc im Header
base64, quoted-printable
Charset

RFC 2183
Content-Disposition
Inline, Attachment, Filename

RFC 2231
Umlaute etc in Parameter
Charset, Sprache
Hex-Encoding
Aufspaltung langer Parameter

Widersprüchliches MIME-Boundary

genua Ein Unternehmen der Bundesdruckerei

```
Content-type: multipart/mixed;
  boundary=bb; boundary=##

This is a multipart message

--bb
Content-type: application/zip;
  name=virus.zip
Content-Transfer-Encoding: base64

--##
UEsDBAoAAAAAAO6Tn0m2hH8nEwAAAB....
AQABAE4AAABVAAAAAAA=
--##--
--bb--
```

Preamble

Daten
base64
virus.zip

Preamble

Daten
Müll

wird i.A. ignoriert von base64 Parsern, da ungültige Zeichen in base64

boundary=bb; boundary=##
Thunderbird, Roundcube, Mutt
Fail: **Snort, Amavisd, FW#2, FW#3**

boundary=##; boundary=bb
Outlook, Apple Mail
Fail: **Snort, ClamAV, FW#1**

Unerwartetes Line-Folding

genua Ein Unternehmen der Bundesdruckerei

```
Content-type: application/octet-stream;
  name=virus.exe
Content-Transfer-Encoding:
<space>
<space>base64

TVqQ...VGhpcyBwcm9ncmFtIGNhbm5vdCBi...
```

legal, aber unerwartet, da keine lange Zeile

MUA sehen base64

Thunderbird
Apple-Mail
Outlook
Mutt
Webmail#1
Webmail#2

Analyse ist blind

ClamAV
FW#1
Webmail#1 AV
Webmail#2 AV
Virustotal 18/34

genua Ein Unternehmen der Bundesdruckerei

- mehrere Content-Transfer-Encoding
  ```
  Content-Transfer-Encoding: base64
  Content-Transfer-Encoding: quoted-printable
  ```
- binäre Daten mit quoted-printable encoden
  diverse FW und AV erwarten dort nichts böses
- nicht-standardisierte CTE verwenden
  uuencode, binhex, yenc, ...
- Boundary mit RFC2231 definieren:
  ```
  Content-type: multipart/mixed; boundary*=''fo%6f
  ```
- leicht kaputtes Base64 und Quoted-Printable verwenden
  Fehler werden unterschiedlich behandelt

genua Ein Unternehmen der Bundesdruckerei

- Testsuite zum Verhalten von MUA, Firewalls, Mail-Filtern, Antivirus ...
  - mehr als 350 Einzeltests
  - getestet mit typischen MUA, Snort, ClamAV, amavisd, einigen kommerziellen FW und einigen Webmailern → alle kaputt
  - diverse Automatismen für SMTP und PCAP, aber nicht voll-automatisch wie HTTP-Evader
  - derzeit nicht öffentlich
    bei Bedarf für Pentesting etc bitte kontaktieren

Zusammenfassung

genua Ein Unternehmen der Bundesdruckerei

- Umgehung von Analysen auf Applikationsebene oft trivial möglich
- Aktive Analyse kann theoretisch durch Bereinigung Angriffe implizit verhindern
  Je konservativer Normalisierung, destso besser
  Braucht entsprechendes Know-how
  Kostet Performance
  Macht evtl. Mailsignaturen kaputt
- Mehr Details, Testserver
  http://noxxi.de/research/http-evader.html
  http://noxxi.de/research/http-evader-testsite.html
  http://noxxi.de/research/semantic-gap.html

Vielen Dank!
Fragen? Oder Bonus-Slides?

genua Ein Unternehmen der Bundesdruckerei

Quelle: gefunden im Internet

Bonus: HTTP Mehrfachkompression

genua Ein Unternehmen der Bundesdruckerei

```
HTTP/1.1 200 ok
Content-Encoding: gzip
Content-Encoding: deflate
```

gzip + deflate	gzip	unkomprimiert
Firefox	Safari	MSIE
Chrome		MS Edge
Opera		

Q4/2015 – 50% Top Enterprise Firewall Fail

Bonus: div HTTP

genua Ein Unternehmen der Bundesdruckerei

```
HTTP/1.1 200 ok
Transfer-Encoding:: chunked
```

~~Chrome~~, **Firefox**, ~~MSIE~~, ~~MS Edge~~, **Safari**, ~~Opera~~

```
HTTP/1.1 200 ok
Transfer-Encoding<space>: chunked
```

Chrome, ~~Firefox~~, ~~MSIE~~, **MS Edge**, **Safari**, **Opera**

```
HTTP/1.1 200 ok
Transfer-Encoding: x chunked
```

~~Chrome~~, **Firefox**, ~~MSIE~~, ~~MS Edge~~, **Safari**, ~~Opera~~

```
HTTP/1.1 200 ok
<space>Transfer-Encoding: chunked
```

~~Chrome~~, ~~Firefox~~, **MSIE**, **MS Edge**, ~~Safari~~, ~~Opera~~

Bonus: HTTP Header-Ende

genua Ein Unternehmen der Bundesdruckerei

```
HTTP/1.1 200 ok\r\n
Content-Encoding: gzip\r\n
<Header-Ende>
```
gzip Payload

\r\n, \n	<space>\n	<space>\n\n	\n\r\r\n
Firefox	~~Firefox~~	**Firefox**	~~Firefox~~
Chrome	~~Chrome~~	**Chrome**	~~Chrome~~
Opera	~~Opera~~	**Opera**	~~Opera~~
Safari	~~Safari~~	**Safari**	**Safari**
MSIE	**MSIE**	~~MSIE~~	**MSIE**
MS Edge	**MS Edge**	~~MS Edge~~	**MS Edge**

Bonus: MIME yenc

yet another encoding – nicht standardisiert – benutzt in Newsgruppen
unterstützt von Thunderbird auch in Mails – Fail: alle FW, Virustotal 31/34

```
From: me
To: you
Subject: [0] multipart-basic-singlepart-x-yencode eicar.zip 2017-04-09 21:35
Mime-Version: 1.0
Message-Id: <86e7be25.69ff.58ea8cfa@example.com>
Content-type: multipart/mixed; boundary=foobar
Content-Length: 610

--foobar
Content-type: text/plain
Content-Transfer-Encoding: x-yencode

=ybegin line=128 size=51 name=file.bin
klmn3Z[\]^g_`abcJJcba`_g^]\[ZJgJg<82><83>J}<99><97><8f>J<97><99><9c><8f>J<9e><8f>¢<9e>4^M
=yend size=51
--foobar
Content-type: application/octet-stream
Content-Disposition: attachment; filename="eicar.zip"
Content-Transfer-Encoding: x-yencode

=ybegin line=128 size=186 name=file.bin
zu-.>*,*2*;t¸sfù{<92>p***n***3***<8f><93><8d><8b><9c>X<8d><99><97>µZ^_<81>6z<9f><9a>6²`³3²´
^<9d><9b>6<9c>û<9f>^^5^[6^]647=@7<9b>78û<9f>^]^^<9b>^?~^[ú=`ú,*zu+,>->*,*2*;t¸s^M
fù{<92>p***n***3**********à«****<8f><93><8d><8b><9c>X<8d><99><97>zu/0****+*+*a***<97>*****
=yend size=186
--foobar--
```

Bonus: MIME Multi- vs. Singlepart

genua Ein Unternehmen der Bundesdruckerei

```
Content-type: multipart/mixed; boundary=foo
Content-type: application/octet-stream
Content-Disposition: attachment;
   filename="eicar.zip"
Content-Transfer-Encoding: base64

UEsDBBQAAgAIABFK....
```

MUA sehen Inhalt	Analyse ist blind
Outlook	FW#1
Mutt	FW#2

Bonus: MIME Base64 = inside

genua Ein Unternehmen der Bundesdruckerei

```
Content-Transfer-Encoding: base64
```

```
Vkk=        <-- VI
UlVTIQ==    <-- RUS!
```

VIRUS!

Thunderbird
Roundcube

blind (VI)

Snort
Amavisd
Clamav
FW#1