

microsoft.public.windowsxp.general: Re: CWS.SEARCHX CoolWebSearch won't go away!

Re: CWS.SEARCHX CoolWebSearch won't go away!

Source:

<http://www.tech-archive.net/Archive/WinXP/microsoft.public.windowsxp.general/2004-05/26049.html>

From: Primax (*primax_at_seggerskeppel.com*)

Date: 05/26/04

Date: 26 May 2004 06:20:36 -0700

The latest CWSshredder didn't work now with CWS.searchx (at least that's how it detected the spyware)

i found following registry entries that re-insert the spyware at IE.

remove those or search for daodn.dll
run CWSshredder
restart

Windows Registry Editor Version 5.00

```
[HKEY_CLASSES_ROOT\CLSID\{D932CFA2-2690-493C-B8B2-4446B2FC32D4}]
[HKEY_CLASSES_ROOT\CLSID\{D932CFA2-2690-493C-B8B2-4446B2FC32D4}\InProcServer32]
@="C:\\WINNT\\System32\\daodn.dll"
"ThreadingModel"="Apartment"
```

```
[HKEY_CLASSES_ROOT\CLSID\{CF32DB60-D35E-4D5F-A622-34EEB0673531}]
[HKEY_CLASSES_ROOT\CLSID\{CF32DB60-D35E-4D5F-A622-34EEB0673531}\InProcServer32]
@="C:\\WINNT\\System32\\daodn.dll"
"ThreadingModel"="Apartment"
```

```
[HKEY_CLASSES_ROOT\CLSID\{0D2BFD8C-D620-4A2F-B264-77C76525633F}]
[HKEY_CLASSES_ROOT\CLSID\{0D2BFD8C-D620-4A2F-B264-77C76525633F}\InProcServer32]
@="C:\\WINNT\\System32\\daodn.dll"
"ThreadingModel"="Apartment"
```

```
[HKEY_CLASSES_ROOT\CLSID\{A7922508-C14A-4D07-A62D-4DDEC39528B1}]
[HKEY_CLASSES_ROOT\CLSID\{A7922508-C14A-4D07-A62D-4DDEC39528B1}\InProcServer32]
@="C:\\WINNT\\System32\\daodn.dll"
"ThreadingModel"="Apartment"
```

If you can't find any daodn.dll try searching all files containing other keywords

Below a piece from the daodn.dll file

Re: CWS.SEARCHX CoolWebSearch won't go away!

microsoft.public.windowsxp.general: Re: CWS.SEARCHX CoolWebSearch won't go away!

```
<div class=searchPanel>
  <form id=formWeb action="http://searchx.cc/search.php" method=get
  target="_main">
  <input type=hidden name="pin" value="13">
  <label for=txtWebSearch>Find a Web page containing:</label><br>
  <input class=inputs type=text name=ww id=txtWebSearch><br>
  <table width=100% cellpadding=0 cellspacing=0 class=searchTable><tr>
  <td class=rightButton><input type=button onclick="$Bx();return null;"
  value="Search" title="Start Searching"></td>
  </tr></table>
  </form>
</div>

<script language=javascript>
function $Bx(){
s=escape(formWeb.ww.value);
if(s==""){
  alert("Please specify something to search for!");
  return;
}
formWeb.submit();
}
function go(text) { formWeb.ww.value=text; $Bx(); }
</script>

<br>

<table border=0 cellpadding=2 cellspacing=0 width=100% height="125"
style="border:1 solid #e53701">
<tr bgcolor="#e53701">
  <td>
  <font color="white"><b>Hot Searches</b></font>
  </td>
</tr>
<tr bgcolor="#e53701">
  <td><br><font style="line-height:12pt;">
  &nbsp;<a class=h href="javascript:go('hydrocodone')">Hydrocodone</a><br>
  &nbsp;<a class=h href="javascript:go('moving companies')">Moving
  Companies</a><br>
  &nbsp;<a class=h href="javascript:go('nevada corporation')">Nevada
  Corporation</a><br>
  &nbsp;<a class=h href="javascript:go('pool cleaning')">Pool
  Cleaning</a><br>
  &nbsp;<a class=h href="javascript:go('recreational vehicle
  insurance')">Recreational Vehicle Insurance</a><br>
  &nbsp;<a class=h href="javascript:go('mortgage refinancing')">Mortgage
  Refinancing</a><br>
  &nbsp;<a class=h href="javascript:go('casino online')">Casino
  Online</a><br>
  &nbsp;<a class=h href="javascript:go('spyware')">Spyware</a><br>
  &nbsp;<a class=h href="javascript:go('adware')">Adware</a><br>
```

Re: CWS.SEARCHX CoolWebSearch won't go away!

microsoft.public.windowsxp.general: Re: CWS.SEARCHX CoolWebSearch won't go away!

 Antivirus

</td>
</tr>
</table>

