Andrew Romatz

From: Daniel Donah [dan@direct-revenue.com]
Sent: Monday, April 04, 2005 1:39 PM
To: Joshua Abram
Subject: FW: Seems like they found athea...

Let's talk about this tomorrow

Begin forwarded message:

From: "Douglas Kee" <daug@direct-revenue.com>
Date: April 4, 2005 1:23:32 PM EDT
To: "Dan Donah" <dan@direct-revenue.com>, "Raffi Minassian" <raffi@direct-revenue.com>, "Chris Dowhan" <chris@direct-revenue.com>, "Redmayt Hoek" <rd@direct-revenue.com>, "Sabish Dhinakaran" <sd@direct-revenue.com>, "Matt Knox" <mknx@direct-revenue.com>
Subject: Seems like they found athea...

http://www.webhelpers4u.com/

Though I'm not sure why they are associating us with a wallpaper download: -
http://www.webhelpers4u.com/nontransponderws/wallpapers4u_4622065.html
WebHelper4U.com and its Adware Popups installations from pacimedia.com

Updated: 02 Apr 2005

Direct from the exotic free wallpaper website in India, Wallpapers4u.com, if you don't have all the up-to-date security, you can set back and enjoy a 36 plus minute installation from a suspected CPM Media site: pacimedia.com. If you are not careful with the popup install boxes or their Windows Media player exploit: wpplayer.exe.tmp. 5kb in size gets into your computer.

Below you will notice that the first install box is the Security Warning where you can click OK, No, or Cancel or hit the Red X but as soon as that the Security Warning box appears you also get the Browser Enhancement Installation dialog box which will not allow you to click no.

What the small box does is drop a file into your temp folder named PFF_*.exe where the * is a random number. Each time the box appears another file will also be dropped into the temp folder. You will also notice that you need to uncheck the Install agreement box and then click the "CLOSE THIS WINDOW" which still if not careful start the installation of 3rd party adware.

Oh, say you uncheck the box and click the close this window button. You then get their next "please install me" tactic.

The second window below is where a toc_*.exe is dropped. This time it states that the user got here because they had previously agreed to the terms. Again you are supposed to uncheck the box and click the close this window.
Browser Enhancer

Congratulations you have been awarded a Browser Enhancement!

Key Features of our Software Include:

1. Giving the user another opinion while they surf the web, broadening their experience and knowledge of the web.
2. Giving options to search the web with great search engines.
3. Providing the user with other partner software free of charge.

You have previously agreed to our Terms and Conditions to get to this step of installation and you can review these terms by clicking right on the link.

If you change your mind and would not like to continue the installation please uncheck the box below and close this window. If you leave the box checked and close this window we will finish your installation free of charge.

C:\ Root and Local Settings Temp folders

<table>
<thead>
<tr>
<th>Name</th>
<th>Program Files Folder</th>
</tr>
</thead>
<tbody>
<tr>
<td>0401[1].exe</td>
<td>Windows media player</td>
</tr>
<tr>
<td>1.exe</td>
<td>Exploit</td>
</tr>
<tr>
<td>1hxp20.dll</td>
<td>windows media player</td>
</tr>
<tr>
<td>20007.exe</td>
<td>exe.tmp</td>
</tr>
<tr>
<td>4241278.dll</td>
<td>70xs0990_newclearsearch.variant.txt</td>
</tr>
<tr>
<td>a95frhe.exe</td>
<td>70xs0990_10189296.txt</td>
</tr>
<tr>
<td>a95frhe.ini</td>
<td>70xs0990_1258770.txt</td>
</tr>
<tr>
<td>nbexe.exe New Transponder File</td>
<td>70xs0990_13459178.txt</td>
</tr>
<tr>
<td>aircity.exe</td>
<td>70xs0990_1692858.txt</td>
</tr>
<tr>
<td>ap22qfd4.dat</td>
<td>70xs0990_19505320.dat</td>
</tr>
<tr>
<td>aj9h4qmo.exe</td>
<td>70xs0990_20234002.bin</td>
</tr>
<tr>
<td>aj9h4qmo.ini</td>
<td>70xs0990_21752643.bin</td>
</tr>
<tr>
<td>ausrp2.dll</td>
<td>70xs0990_26413025.bin</td>
</tr>
<tr>
<td>authrootsql[1].txt</td>
<td>70xs0990_37353732.exe</td>
</tr>
<tr>
<td>authrootsql[1].cab</td>
<td>70xs0990_38663579.txt</td>
</tr>
<tr>
<td>auto_update_uninstall.exe</td>
<td>70xs0990_4164622.txt</td>
</tr>
<tr>
<td>auto_update_uninstall.log</td>
<td>70xs0990_45129992.dat</td>
</tr>
<tr>
<td>banner[1]</td>
<td>70xs0990_48837544.dat</td>
</tr>
<tr>
<td>baur55q9.dat</td>
<td>70xs0990_49055445.dat</td>
</tr>
<tr>
<td>ibdil[1].cab</td>
<td>70xs0990_5297844.bin</td>
</tr>
<tr>
<td></td>
<td>70xs0990_5555544.bin</td>
</tr>
</tbody>
</table>

http://www.webhelper4u.com/nontransponders_wallpapers4u_2220231.html

1/10/2006

Now for the best part, after 30 minutes and going over the whole computer to get as many files as possible, below is a list files that came out for the infestations.
Windows Media Player wmpplayer.exe.tmp Exploit

Finally found where the wmpplayer.exe.tmp exploit file came from and the file that created it!

pan-advert.com/ads/banners/inst25.exe - This is the wmpplayer.exe.tmp

inst25.exe 3kb
wmpplayer.exe.tmp in windows media player folder
code:
\adinstallwin32.exe - system32\adinstallwin32.exe SystemRoot\win\alwaysupdatednews.com\terms\toc_0052.exe

**
inst25.exe 5kb in Temp Internet files folder
code:
\adinstallwin32.exe - system32\adinstallwin32.exe SystemRoot\win\alwaysupdatednews.com\terms\toc_0052.exe

Back up to File List  Back to the Top

Now pan-advert.com has an email to aviatbiz.com and the address in the whois for aviatbiz.com is the same address is the whois for pacimedia.com.

Whois Data
pan-advert.com 213.159.119.4
Registrant:
Sea Media S.A. Sea Mediz S.A. seamedia @aviabiz.com:
Sea Media S.A.
P.O. Box 1987 9A
Panama NONE NA

PA
507-575-6771
Domain Name: pan-advert.com
Admin Contact:
Zarya Econsulting Corp. Zarya Econsulting Corp. info@aviabiz.com
P.O. Box 1987 9A
Panama NA
PA
507-575-6771
Technical Contact:
Sea Media S.A Sea Media S.A info@aviabiz.com
Sea Media S.A
P.O. Box 1987 9A
Panama NA
PA
507-575-6771
Billing Contact:
Sea Media S.A Sea Media S.A info@aviabiz.com
Sea Media S.A
P.O. Box 1987 9A
Panama NA
PA
507-575-6771
Record created on Jan 4 2005.
Record expires on Jan 4 2006.
Domain servers:
ns1.pan-advert.biz
ns2.pan-advert.biz

pscmidia.com 213.159.119.18
Domain name: pscmedia.com
Administrative Contact:
- Tomaz Urbic pacerdltd@yahoo.com
  1.2069844492
Fax: -
  Trinity House 1st Floor
  Albert Street PO BOX 1402
  Victoria MAHE N/A
SC
Billing Contact:
- Tomaz Urbic pacerdltd@yahoo.com
  1.2069844492
Fax: -
  Trinity House 1st Floor
  Albert Street PO BOX 1402
  Victoria MAHE N/A
SC
Technical Contact:

http://www.webhelpers4u.com/nominalpanders/wallpapers4u_4022001.html