

# McAfee VirusScan installer uses insecure ActiveX controls

*Source:* <http://www.derkeiler.com/Mailing-Lists/NT-Bugtraq/2004-04/0031.html>

---

*From:* Jonathan Payne ([jpayne\\_at\\_DSL.PIPEX.COM](mailto:jpayne_at_DSL.PIPEX.COM))

*Date:* 04/25/04

Date: Sun, 25 Apr 2004 08:17:25 +0100  
To: NTBUGTRAQ@LISTSERV.NTBUGTRAQ.COM

After installing the McAfee VirusScan, it appears that it is possible for any web page to access the Windows registry with the following HTML:

```
<html>
<object classid="clsid:4C29D864-C55A-46DD-865C-17A1B7CC1A1A" id="gobjReg"
style="display: none;">
</object>
<h1>McAfee installer test</h1>
<script language="vbscript">
document.write( _
gobjReg.RegQueryValue( "HKCU\Control Panel\Desktop", "Wallpaper") _
)
</script>
</html>
```

(when viewed in IE 6 with default security and with VirusScan installed, this HTML displays the location of the current Windows desktop bitmap)

You can see this behaviour by selecting the 15-Day Free trial of McAfee Virus scan from this page:

<http://download.mcafee.com/us/eval/evaluate2.asp?cid=9445>

Then going through the account creation process and then clicking on the download link.

The download page (the one with the "Start" button) appears to install a number of ActiveX controls which are not secured in any way. As well as the registry one, there are controls for accessing the file system and for configuring the operating system.

I have uploaded a full copy of the IDL for the installer objects here:

<http://www.aslg21.dsl.pipex.com/test/McAfeeIDL.txt>

There appear to be lots more fun interfaces that I haven't tested yet.

Jonathan Payne

## NT–Bugtraq: McAfee VirusScan installer uses insecure ActiveX controls

-----  
Earn up to 10 credit course hours toward the TruSecure ICSA Practitioner (TICSA) Credential and receive a TICSA exam coupon by attending the Infosecurity Canada 2004 conference. Featured speaker, Marcus J. Ranum, TruSecure inventor of the proxy firewall will present on June 3 at 11:30 AM. Visit <https://ticsa.trusecure.com> for certification details and <http://www.infosecuritycanada.com> for conference information. Become TICSA certified and see what happens!  
-----