From: David Cole
Sent: Friday, April 11, 1997 8:03 AM
To: Michael Toutonghi
Subject: RE: Another security hole, using well-intentioned third party control

I am a big big fan of signing sites. as a user, I don't want to make a trust decision any more granular than that.

-----Original Message-----
From: Michael Toutonghi
Sent: Thursday, April 10, 1997 7:00 PM
To: Philip Bogle; Ben Slivka, Robert Welland; Cornelius Willis, Bob Atkinson (Exchange)
Cc: Chris Jones, Sam McKelvie, David Cole, Mike D Smith, Charles Fitzgerald, John Ludwig; Brad Silverberg
Subject: RE: Another security hole, using well-intentioned third party control
Importance: High

I really believe that our only answer to this stuff is going to be sandboxed controls and signing of HTML & sites. SamMck and RobWell did a lot of thinking on these issues last year, and after discussing the signed script problem with Sam, I'm also convinced that it's the HTML & sites that need to be signed. We can still provide the capability support we've discussed, but just signing script as Netscape is doing will not protect us (or them) from these kinds of HTML->Script->Java->Control attacks.

We have a meeting on this tomorrow morning with the script/trident folks. I think we should put a lid on these issues for now until we've got a solid answer.

Philip, can you restrict the addressees of your mail to those on the "to/cc" line of this mail? Ideally, a smaller set would be better. You can always knock on my door :-)

Thanks,

Mike

-----Original Message-----
From: Philip Bogle
Sent: Thursday, April 10, 1997 5:42 PM
To: Ben Slivka, Robert Welland, Cornelius Willis, Bob Atkinson (Exchange)
Cc: Michael Toutonghi, Chris Jones
Subject: Another security hole, using well-intentioned third party control
Importance: High

I already mentioned the hazards of the signed Net-Installer control that you can find at www.activex.com, which is incorrectly marked safe for initializing for untrusted data.

I've created a nasty demo of the harm that can be done using the well-intentioned control at:

file://\\philbo\root\netinst\hack.htm

This page masquerades as the install page for the control and initializes the control with data that causes it to:

- Set IE's security settings to none by munging the registry
- Install a Java class file to the trusted Java\Classes directory.
- Install and run a program that causes the computer to restart

You might think that this is no different from the Internet Exploder control. But there really is a fundamental difference. The control author in this case had no malicious intent-- he just made an error in judgement that opened up the control to exploitation by other people. Also, because of the way I've structured the page, I make it look like the control is to blame for anything bad that happens, rather than the page that misuses it. Finally, the control is referenced by a well-known (and presumably trustworthy) repository of ActiveX controls.

If an outside party discovers this control, they can use it to support the argument that the responsibility that ActiveX forces on a control author is too high-- they'll say everyday developers shouldn't have to make decisions

that could undermine the security of the whole system, that responsibility should be centralized in a sandbox system. I can't say I entirely disagree with them.

Also, this case raises troubling questions about how we fix the issue. Since the author had no ill-intent, it will look bad for Microsoft to lean on him with the lawyers. I forsee many similar situations in the future if we don't have a better policy for certifying or sandboxing controls.

-phil

-----Original Message-----
From: Philip Bogle
Sent: Thursday, April 10, 1997 10:29 AM
To: Philip Bogle
Subject: FW Serious security holes in ActiveX controls for MSN (and elsewhere)
Importance: High

From: Philip Bogle[FAX:+1 (206) 881-8095]
Sent: Thursday, April 10, 1997 6:20 AM
To: Robert Welland; Ben Slivka; Chris Jones
Cc: Michael Toutonghi; Cornelius Willis; Brad Schick; Larry Sullivan
Subject: Serious security holes in ActiveX controls for MSN (and elsewhere)
Importance: High

After hearing about the security hole in the Norton navigator control, I decided to review the security of other ActiveX controls likely to be preinstalled on users machine.

What I found is pretty shocking-- developers often sign and publish inherently unsafe or incorrectly marked controls, and Microsoft is one of the worst offenders.

Consider MSN, for example. It preinstalls several powerful and unsafe controls, nonetheless marked "Safe for Scripting". I created several web pages (attached below) that use these controls to munge the registry and accomplish other evils . Regardless of security settings, the MSN user gets absolutely no warning or chance to reject the controls before the damage is done (because MSN preinstalls them.)

Even without scripting, many controls are inherently dangerous. In a brief search of www.activex.com, I found three signed controls with the ability to run arbitrary unsigned code on the users machine without requiring any scripting and without any warnings to users. I have attached descriptions of these controls below.

Norton was not an isolated incident. We really have a general problem-- ActiveX control developers are behaving extremely naively with respect to security. They are creating signed controls with automated capabilities far too dangerous for general internet use, or marking controls "Safe for Scripting" that clearly shouldn't be, despite the pains we took to explain the meaning of that concepts At this rate, ActiveX is going to gain an extremely bad reputation

Below are the descriptions of the insecure controls ..

MSN Registry Control
The web page below uses the "MSN Registry Control" (!!!) to inspect and modify keys in the various MSN subtrees of the registry. (It doesn"t allow arbitrary registry munging, but even the current capability is enough to cause serious trouble.) The example I created displays and/or deletes the MSN registry entries that list the URLs that the user has typed in
<< File: hack-msn >>
A script using the control could do many more evil things: render components of MSN unusable by blowing away the appropriate registry entries, substitute a bogus stock server for the real one, fill up the users hard drive by creating registry keys ad infinitum, etc.

MSN Mail Control
This page uses the MSN mail control to obtain the user ID (which it could send back to the server) and to launch mail.

<< File hack-mail >>
Active Data Connecter (possibly dangerous)

The Active Data Connector is marked "Safe for Scripting", and appears to allow a script on an untrusted page to connect to a database behind a firewall (as long as its not password protected) and siphon data out of it. I didn't come up with an example page, but someone who knows more about the ADC should think carefully about this

Below are controls that are dangerous even without scripting, which I found on www.activex.com.

DataRamp Assistant
"The DataRamp Assistant makes it easy to embed application references in World Wide Web pages. When a user clicks on a Web page, the DataRamp Assistant ActiveX control automatically downloads the application definition files, configures the required data source, and launches the application"

http://www.activex.com/PC/Result/TitleDetail/0,16,0-15818,00.html

Net-Installer
This controls allows programs to download and run automatically on the users machine

http://www.twenty.com/Pages/NI/NIDTK.shtml

App-launcher
This control supports the ability to launch arbitrary apps without user intervention.

http://www.activex.com/PC/Result/Download/0,27,0-22413,00.html