

## Re: 030 igetnet ignkeywords

**Source:** <http://www.derkeiler.com/Mailing-Lists/securityfocus/incidents/2002-11/0097.html>

---

**From:** Nick FitzGerald ([nick@virus-1.demon.co.uk](mailto:nick@virus-1.demon.co.uk))

**Date:** 11/16/02

Date: Sun, 17 Nov 2002 11:34:46 +1300  
From: Nick FitzGerald <[nick@virus-1.demon.co.uk](mailto:nick@virus-1.demon.co.uk)>  
To: [incidents@securityfocus.com](mailto:incidents@securityfocus.com)

"Waitman C. Gobble" <[waitman@emkdesign.com](mailto:waitman@emkdesign.com)> wrote:

> *Couple of things to note. The file is signed by IGetNet, LLC using a  
> Verisign cert. I suppose that signed applications are always  
> trustworthy?*

No. By default IE ships with no "trust always" certificates and the "Internet zone" is set to enable download of signed ActiveX controls but not of unsigned ones (that's a mal-description too -- it has to "downlaod" the control to find out if it is signed or not... What they mean is consider offering the control for execution once it is downloaded). Further, the default config for the Internet zone is to run ActiveX controls. In practice this means once a control is downloaded and determined to be properly signed, IE will prompt you for whether you trust the signer in this instance \_and\_ it gives you an option to automatically (i.e. without prompting you again) trust anything else signed with the same certificate (note that is not the same thing as trusting anything esle signed by the same developers \_or claiming to be signed by the same developer\_ -- a developer with two different product lines could easily have two certificates, using one for each and permanently accepting one would still cause prompts for the other, even though the name on the certs might be identical).

I know MS likes making its products easy to use, and heaven knows MS understands that is a large part of its relative success, but offering the "always accept" option, \_at least on software running on "corporate quality" OSes such as Win2K and XP Pro is a bad design choice. You'd have thought something inside MS would have learnt something from the Office macro virus holocaust which raged incessantly \_despite\_ MS giving user options to disable macros in documents, but it seems not. Perhaps in the new, enlightened age of "Trustworthy Computing" in which MS product designers and developers now work, this will change?

Of course, committed system admins have had the "only allow admin-approved controls" options for a little while now, but I suspect that

few actually use it.

- > *I realize the obvious painful answer is that it was installed by*
- > *clicking on a link on a web site, and allowing it to install HOWEVER –*
- > *everyone I have heard from has NO recollection of doing such a thing.*

Rule number one — never believe your users \_denials\_ of doing soemthing. "How did this keyboard get full of coffee?" "I don't know" Like, you expect they are going to say "I'm a klutz and spilled it" or "I deliberately sabotaged it"??

Get real.

As someone else has posted, users are far too accustomed to answering "Yes", "OK" or "Accept" to mumbo–jumbo tech/geek speak they do not understand as part of their normal use of this wonderful new technology. Further, far too many of them have had too many experisnces of saying "No" or "Cancel" and then things not working properly that they are \_conditioned\_ to accepting things.

We have just seen the "Friend Greetings" "eCard viewer" issue, where right up front, right at the top of the EULA screen when installing the "viewer" the user is told that installing the s/w will cause it to send Email to all the addresses in their Outlook address books. Do they click the "Accept" button or do they click "Don't Accept" and/or do they call their internal tech suupport/helpdesk/IT staff/ etc?? Well, we don't know how many click "Don't Accept" but few have called their IT folk and we know thousands are clicking "Accept".

Why?

Are they stupid? Well, a few surely are, but most have been conditioned to accepting whatever their machine throws at them because historically not doing so has interfered with their "successful" use of the machines.

Facing this self–evident truth, what are vaguely sane system admins to do? Well, first, they should find an OS and/or application set that allows them to prevent the users shooting themselves in the feet. Unfortunately, no popular OS and application set that allows this has been prodcued. Why? Because the designers of the popular Oses and applications, who have been rewarded with apparently never–ending sales and upgrade orders (though they are now showing signs of recognizing there is a final carriage on the gravy train and they are closer to it than they originally projected) have not produced products that allow admins to take such control, or if they do, the overhead of obatining nad maintaining that control is prohibitive.

- > *IMO This thing behaves like a sticky virus, it mysteriously gets*
- > *installed on the machine, ...*

## SecurityFocus Incidents: Re: 030 igetnet ignkeywords

Well, you don't know that for sure. You have users who say they did not install it, but if you actually had serial screen shots of their machines from each window redraw, I suspect you'd have a different "picture"...

- > ... and seems to be difficult to remove. Chris
- > Wagner kindly posted a link on this page to removal instructions that seem to work, however one person telephoned me last night and indicated that the conditions persist even after following the instructions.

I have not tried removing it on a machine with an active Internet connection, so my experience may be different, but the uninstaller IGetNet provide did appear to "sufficiently" remove the thing from my test machine (it left an unregistered DLL, but got rid of the rest).

- > I haven't heard anyone making the claim that the "browser upgrade" from IGetNet is useful, in fact everyone I have heard from is upset about it and from wants it permanently removed from their system as quickly as possible.

Same here...

- > It brings to my mind the term "viral marketing".

Yep, and although not technically a virus, it is the sort of thing that the antivirus, anti-Trojan and anti-adware/spyware folks are increasingly being pressured to detect and provide reliable removal of. I suspect the more "aggressive" viral marketers have badly misjudged userland's acceptance or tolerance for such things.

- > In my opinion IGetNet wants to come into the picture, apparently through the back door, as a replacement for RealNames. I am not sure that enough, if any, people would actually buy keywords from them. After losing close to \$1200 US when RealNames got its plug pulled, I wouldn't touch IGetNet with a ten foot pole.

8-)

And the more bad publicity like this you can generate for them the better...

- > I have a hunch that this is coming in through a program that does unattended (or attended for that matter) automatic updates, or a program that routinely gets stuff off the Internet, like a music player.

This is, of course, quite possible and what got some of the other "adware" folk in trouble. I forget precisely who now, but one of the adware company's "products" was supposed to always ask permission and display a list of actions the software took, the company's privacy policy and so on. However, some of their clients who bundled it with their own software took the basic installer script and after

SecurityFocus Incidents: Re: 030 igetnet ignkeywords

displaying just their own EULAs, etc (which did not mention the specifics of the adware, or in some cases even that the adware was included) then installed their own s/w and the adware. The IGetNet "add-in" could easily be installed "silently" in such a way.

- > *Additionally, I imagine any day now the phone will start ringing off the*
- > *hook from our clients that have mysteriously contracted the virus and*
- > *seek removal.*

Caveat emptor.

Their stupidity is a further marketing opportunity for you. (Of course, if you find that distasteful, you should be recommending they overhaul their systems so that better administrative control is available and such "abuse" prevented, rather than needing continual clean up after the fact...).

- > *My guess is that this is the tip of the iceberg – bigger better faster*
- > *harder is certain to come.*

Such is the way of things, it appears...

--

Nick FitzGerald  
Computer Virus Consulting Ltd.  
Ph/FAX: +64 3 3529854

---

This list is provided by the SecurityFocus ARIS analyzer service.  
For more information on this free incident handling, management  
and tracking system please see: <http://aris.securityfocus.com>