

Re: E-Mail received – Anyone Else affected?????

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.security/2003-05/0682.html>

From: Susan Bradley, CPA aka Ebitz – SBS Rocks [MVP] (*sbradcpa_at_pacbell.net*)

Date: 05/13/03

Date: Mon, 12 May 2003 20:20:24 -0700

To: deb0822@cs.com

Hoax. Don't load this

>From SANS:

We received a few reports of e-mails advertising the 'quick launch' spyware as an anti virus tool. A typical e-mail reads:

Subject: Windows Update Notification

WINDOWS SECURITY WARNING!!

A VIRUS HAS BEEN DETECTED ON YOUR COMPUTER. IN ORDER FOR YOUR COMPUTER NOT

TO CRASH YOU WILL NEED TO GO TO:

<http://WWW.WINDOWSUPDATENOW.COM>

AND IT WILL AUTOMATICALLY UPDATE YOUR COMPUTERS SECURITY PATCHES.

SIMPLY TYPE IN <http://WWW.WINDOWSUPDATENOW.COM> INTO YOUR BROWSER.

OTHERWISE

YOU WILL KEEP RECEIVING THIS SECURITY ALERT EMAIL EVERY DAY

Note the use of a 'plausible' domainname: windowsupdatenow.com

**This domain does not belong to Microsoft:

(This Domain is For Sale)

Joshuathan Investments, Inc.

62 Cleghorn Street

Belize City, Belize none

US

microsoft.public.security: Re: E-Mail received – Anyone Else affected?????

Domain Name: WINDOWSUPDATENOW.COM

Administrative Contact –

This Domain Is For Sale – joshuathaninvest@aol.com
(This Domain is For Sale) Joshuathan Investments, Inc.
62 Cleghorn Street
Belize City, Belize none
US
Phone – 501-2-31244
Fax – 501-2-34222

Technical Contact –

This Domain Is For Sale – joshuathaninvest@aol.com
(This Domain is For Sale) Joshuathan Investments, Inc.
62 Cleghorn Street
Belize City, Belize none
US
Phone – 501-2-31244
Fax – 501-2-34222

Once you enter on this page it will redirect you to another URL
(<http://www.quicklaunch.com/perl/detection.pl>).

When visiting the URL, it will attempt to install the quicklaunch
toolbar (<http://download.quicklaunch.com/quicklaunch154.cab>), a known
spyware program.

Removal instructions are available here:

<http://www.doxdesk.com/parasite/BrowserAid.html>

Deb wrote:

> *Received the following e-mail:*
>
> *Subj: Windows Update Notification*
> *Date: 5/12/2003 7:29:12 PM Pacific Standard Time*
> *From: windowsupdate@windowsupdatenow.com*
> *Received from Internet: click here for more information*
>
> **WINDOWS SECURITY WARNING!!**
>
> **A VIRUS HAS BEEN DETECTED ON YOUR COMPUTER. IN ORDER FOR**
> **YOUR COMPUTER**
> **NOT TO CRASH YOU WILL NEED TO GO TO:**
>
> **<http://WWW.WINDOWSUPDATENOW.COM>**
>
> **AND IT WILL AUTOMATICALLY UPDATE YOUR COMPUTERS SECURITY**
> **PATCHES.**
>
> *Subj: Windows Update Notification*

Re: E-Mail received – Anyone Else affected?????

microsoft.public.security: Re: E-Mail received – Anyone Else affected?????

> *Date: 5/12/2003 7:29:12 PM Pacific Standard Time*
> *From: windowsupdate@windowsupdatenow.com*
> *Received from Internet: click here for more information*
>
> *WINDOWS SECURITY WARNING!!*
>
> *A VIRUS HAS BEEN DETECTED ON YOUR COMPUTER. IN ORDER FOR*
> *YOUR COMPUTER*
> *NOT TO CRASH YOU WILL NEED TO GO TO:*
>
> *<http://WWW.WINDOWSUPDATENOW.COM>*
>
> *AND IT WILL AUTOMATICALLY UPDATE YOUR COMPUTERS SECURITY*
> *PATCHES.*
>
> *SIMPLY TYPE IN <http://WWW.WINDOWSUPDATENOW.COM> INTO YOUR*
> *BROWSER. OTHERWISE*
> *YOU WILL KEEP RECEIVING THIS SECURITY ALERT EMAIL EVERY DAY.*
>
> *Thought this was pretty interesting. Anyone else getting it?*
> *Deb*
> *deb0822@cs.com*