

## RE: New Trojan?

**Source:** <http://www.derkeiler.com/Mailing-Lists/securityfocus/security-basics/2004-07/0004.html>

---

**From:** Rivera Alonso, David ([drivera\\_at\\_iberdrola.es](mailto:drivera_at_iberdrola.es))

**Date:** 06/30/04

To: 'Jeff' <[Jeff@Not\\_A\\_Real\\_Address.com](mailto:Jeff@Not_A_Real_Address.com)>, [security-basics@securityfocus.com](mailto:security-basics@securityfocus.com)  
Date: Wed, 30 Jun 2004 13:56:10 +0200

Dear friend,

I had a problem last week with a kind of trojan that was not removed/detected by Spybot S&D, AdAware nor PestPatrol. It is very specific, and had to be removed with CWS shredder (<http://www.spywareinfo.com/~merijn/>). Why don't you try this little tool?

GOOD LUCK,

DAVID

By the way: after this happening, I decided to move to Mozilla family SW, too :-)

-----Mensaje original-----

De: Jeff [[mailto:Jeff@Not\\_A\\_Real\\_Address.com](mailto:Jeff@Not_A_Real_Address.com)]

Enviado el: lunes, 28 de junio de 2004 21:15

Para: [security-basics@securityfocus.com](mailto:security-basics@securityfocus.com)

Asunto: New Trojan?

PLEASE READ ... I feel violated and need much help, if not for the PC, for my nerves.

The PC is a WinXP box, fully patched, routinely checked with Spybot 1.3 and AdAware 6. I run SpywareBlaster as well. I also use Thunderbird 0.6 and Firefox 0.8. All other family members run Thunderbird on this box. IE6 has not been removed but is fully patched.

Norton Antivirus Corporate Edition 9.0, AV file 6/25/2004 r19 is running. (I purposely purchased the licenses at work for our home users also so that they WOULD stay up to date -- a practice I learned from Sprint a long, long time ago.)

I use a Netgear FVS318 to interface to my Verizon DSL account.

## SecurityFocus BASICS: RE: New Trojan?

The events as they happened.

1. My son read his email via the web. It included e-cards. He read them. Doesn't remember where they took him, nor does he remember if he used IE6 or Firefox.
2. Long screaming session about things TO do and things NOT to do while on the internet. 278th time. Disabled his account.
3. Mis-typing a URL will now take me automatically to [www.netidentity.com](http://www.netidentity.com) with the mistaken URL clearly identified inside. Identical results on IE6 and Firefox. Java and Javascript are disabled on Firefox. I leave IE6 alone because I use it when I absolutely must go to some bogus activex site, oh, and windowsupdate. But I don't use it otherwise. I always use Firefox.

URLs that caused this include: mapblast, mapquest, abc, def ... through xyz.

Please note: I had typed "mapblast" but had hit Enter rather than Ctrl-Enter, by mistake. The URLs entered are literally those listed, just the word.

They are then transformed to <http://mapblast/>

4. SAV CE, Spybot, AdAware, SypwareBlaster were all checked for updates and the entire system was scanned. Nothing found.  
  
\*\* My immediate thought was that Network Solutions was up to their  
\*\* old tricks with it's Site Finder business. A quick check of  
\*\* another PC in the house eliminated that.
5. I checked my syslogs and NULL routed the IP address being used to access [www.netidentity.com](http://www.netidentity.com). The same page comes up sans the graphics and the flash. The web page is still there though, just looking sad. Another check of the syslogs brings up 64.15.175.5 as generating the pages, an open proxy.
6. Also ran HiJackThis and went through ALL of the items on it. Nada. Couldn't find the IP addresses or domain names in the registry. I also ran them in reverse notation. Nada.
7. Checked my network settings to make certain that some new DNS server wasn't stuck in. Nope, still set to use the Netgear box. Put 4 different DNS servers in — still get that stupid site.
8. That was all at lunchtime. Haven't had a chance to run netstat or Ethereal to gain any additional clues.

ZOIKS!!!

RE: New Trojan?

SecurityFocus BASICS: RE: New Trojan?

The PC is off. But NOT knowing what is going on is driving me insane.

So while I <ahem> work this afternoon, I thought I would see if any of this sounds, smells or <insert fav sense here> like anything that anyone has seen before!

Jeff

---

Ethical Hacking at the InfoSec Institute. Mention this ad and get \$545 off any course! All of our class sizes are guaranteed to be 10 students or less to facilitate one-on-one interaction with one of our expert instructors. Attend a course taught by an expert instructor with years of in-the-field pen testing experience in our state of the art hacking lab. Master the skills of an Ethical Hacker to better assess the security of your organization. Visit us at: [http://www.infosecinstitute.com/courses/ethical\\_hacking\\_training.html](http://www.infosecinstitute.com/courses/ethical_hacking_training.html)

---

=====

Este mensaje se dirige exclusivamente a su destinatario. Puede contener informacion confidencial sometida a secreto profesional o cuya divulgacion este prohibida, en virtud de la legislacion vigente. No esta permitida su divulgacion, copia o distribucion a terceros sin la autorizacion previa y por escrito de Iberdrola. Si ha recibido este mensaje por error, le rogamos nos lo comuniquen inmediatamente por esta misma via y proceda a su destruccion.

This e-mail is intended exclusively for the individual or entity to which it is addressed and may contain confidential or legally privileged information, which may not be disclosed under current legislation. Any form of disclosure, copying or distribution of this e-mail is strictly prohibited, save with written authorisation from Iberdrola. If you have received this message in error, please notify the sender immediately by e-mail and delete all copies of the message.

=====

---

Ethical Hacking at the InfoSec Institute. Mention this ad and get \$545 off any course! All of our class sizes are guaranteed to be 10 students or less to facilitate one-on-one interaction with one of our expert instructors. Attend a course taught by an expert instructor with years of in-the-field pen testing experience in our state of the art hacking lab. Master the skills of an Ethical Hacker to better assess the security of your organization. Visit us at: [http://www.infosecinstitute.com/courses/ethical\\_hacking\\_training.html](http://www.infosecinstitute.com/courses/ethical_hacking_training.html)

---