

## Re: Re(2): Possible new virus?

**Source:** <http://www.derkeiler.com/Mailing-Lists/securityfocus/security-basics/2003-09/0550.html>

---

**From:** Sebastian Schneider (*ses\_at\_straightliners.de*)

**Date:** 09/11/03

To: "Wilcox, Stephen" <StephenWilcox@universalcomputersys.com>, "Lee Rich" <lee.rich@wlga.gov.uk>

Date: Thu, 11 Sep 2003 22:46:36 +0200

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA1

Hey, this is quite good an idea ; ) I guess as Matt already said, he had no real hands-on yet. Anyways if he's going to take a "sight" seeing tour there're quite a lot of things to be checked. As far as I recall, he didn't say, that those machines didn't boot up as usual.

1 – So first thing's when does that message appear? After POST before starting up the operating system? Or before/after ?

2 – What happens when booting from any bootable CD or just switching off the hard disks in BIOS? Same message? (I guess that's much easier than disconnecting the harddrive physically and the actual owner feels much more comfortable).

3 a – Assuming message still appears, is the fan working properly? What about the CPU temperature? Too hot or within normal range? What does the BIOS tell about the temperatures, if at all?

3 b – Message is not displayed, so it must be some code executed while booting from disk. That code might be executed when running the boot routines in MBR or partition's boot sector or while starting the operating system (I guess Matt said, there were no strange entries neither in config.sys nor in autoexec.bat). Now a linux system is really helpful in doing some forensics ;–)

3 b1 – Check out the startup files like config.sys, autoexec.bat, win.ini, system.ini and the registry entries. Keep an eye on modification dates of the files and compare filesizes to original sizes, maybe MD5 hashcodes. Anything strange?

3 b2 – Assuming nothing found, take a copy of the MBR and bootsector. The tool debug (if not running linux to do that) is quite helpful in such situations. This is not sufficient for later analysis however, since the real code can be in any sectors on the hard disk. Now the boot code needs to get analyzed. Boot block structure is needed, to extract the actual

## SecurityFocus BASICS: Re: Re(2): Possible new virus?

code out of all that informations.

4 – Assuming message still shows up though fan is working, now it might still be a hardware defect, a bug or a virus infecting the BIOS software. If the BIOS shows the temperatures, issue is easier to analyze.

4 a – BIOS says, temperatures are okay. There's no hardware defect, maybe no software bug. Try resetting the BIOS to default values. Message still appears? Has the mainboard a jumper to protect from flashing the BIOS by mistake? Is that jumper set to protect or to allow flashing? If no jumper exists to control flashing, what is set in the BIOS? Is there an option at all?

4 a1 – Jumper or BIOS is set to deny flashing. Most likely, there's some defective hardware.

4 a2 – There's not option to control flashing. Maybe software in flash is buggy, corrupt or changed.

4 b – BIOS provides no way to check system temperatures. So try a third-party tool if available.

5 – In any case of 4 try to obtain the latest BIOS software and try flashing. Don't forget to take a image before overwriting.

5 a – Flashing is denied. Maybe you can't flash at all or a virus might block such nasty things (this is quite hard to code...). Most likely, flashing is not possible due to any restrictions. Check up 4a again. If everything's okay, there might be some malicious code. Analyze the image or verify your steps.

5 b – Flashing is possible and successful. After flashing the message still shows up? So there's some hardware failure or jump to 3b above. If that message doesn't appear this time, old flashed software might be buggy or contains malicious code. Analyze image.

Hope these steps were right and harmonious. Please let me know, if anything's missing or wrong.

Sebastian

On Thursday 11 September 2003 20:48, Wilcox, Stephen wrote:

- > *Ok, I'm sure everyone has an opinion about Chris's original email. It was*
- > *his opinion on where he felt this email belonged, nothing more. The*
- > *administrators of the mail list felt it could fall under this group so here*
- > *it stays. It seems to me everyone is getting off track. Get back into*
- > *focus and use this list for what it's intention is for. Help pointing*
- > *people towards their resolution. I see more and more people wanting to run*
- > *someone through the mud on their opinion then time spent on the issues of*
- > *the original post.*
- >
- > *With that said...*
- >

Re: Re(2): Possible new virus?

SecurityFocus BASICS: Re: Re(2): Possible new virus?

> *I would take a road trip and verify the machines sounds and entirety is in*  
> *fact "Good Working Condition".*  
>  
> *Run the test as some have pointed out.*  
>  
> *It much harder to correctly resolve issues when it comes from a third*  
> *party.*  
>  
> *I wish you good luck in your search for resolution to you problem*  
>  
> *Stephen*  
> *R&D Systems Network Specialist*  
>  
>  
>  
> -----Original Message-----  
> *From: Lee Rich [mailto:lee.rich@wlga.gov.uk]*  
> *Sent: Thursday, September 11, 2003 4:08 AM*  
> *To: security-basics@securityfocus.com*  
> *Subject: Re(2): Possible new virus?*  
>  
>  
> *Chris, in a later posting, Matt has stated that 'another' machine has been*  
> *reported to have the same symptoms; these machines may be just a small*  
> *handful of machines who have the same problem but have not been reported*  
> *yet due to the area covered by 'Internet' Technical support.*  
>  
> *Also, the idea that the message and beeping may be a red herring should not*  
> *be cast aside. For all these systems to suffer the same fault despite*  
> *manufacturer or warranty state. Seems a little iffy to me and I wouldn't be*  
> *surprised if there is actually nothing wrong with the cooling system.*  
> *Saying it's a hardware problem would assume that each firmware reports an*  
> *identical message for the problem. Not to mention that some firmware may*  
> *not even be able to report such an issue.*  
>  
> *-Lee Rich*  
> *security@wlga.gov.uk*  
>  
> -----Original Message-----  
> *From: Chris Berry <compjma@hotmail.com>*  
> *To: security-basics@securityfocus.com <security-basics@securityfocus.com>*  
> *Sent: 10/09/2003 23:51*  
> *Subject: Re: Possible new virus?*  
>  
>  
> *From: "Lee Rich" <lee.rich@wlga.gov.uk>*  
>  
> > *"I'm not sure how it made it on to the list"*  
> >  
> > *And please don't forget, this is 'security-basics'.. which means to me,*  
> > *that it's not all security experts*

Re: Re(2): Possible new virus?

SecurityFocus BASICS: Re: Re(2): Possible new virus?

- > >here, it's people breaking into the field aswell. So you should expect
- > >questions that may be simple to
- > >yourself, but to others, it's part of a learning curve.
- >
- > Oh, I wasn't complaining because it was basic, I was complaining because
- > it's not a security issue. To the best of my knowledge (which on this
- > particular subject is fairly extensive since I'm originally from a hardware
- > background), there is no possible way for software to interfere with the
- > CPU cooler no matter how malicious it is, there just isn't any interface.
- > (though I suppose if you had a motherboard with variable fan speed control
- > and you somehow got an infected firmware update for your BIOS, then maybe,
- > but thats a real long shot) However, as always I'm willing to fess up if
- > I'm wrong, is there anyone here who knows differently? I'd be happy to
- > help the original poster, I was just trying to point out that this isn't
- > the correct forum for hardware questions.
- >
- > Chris Berry
- > compjma@hotmail.com
- > Systems Administrator
- > JM Associates

> "Conciousness: that annoying time between naps."

> \_\_\_\_\_  
> Get a FREE computer virus scan online from McAfee.  
> <http://clinic.mcafee.com/clinic/ibuy/campaign.asp?cid=3963>

- 
- > Captus Networks
  - > Are you prepared for the next Sobig & Blaster?
  - > – Instantly Stop DoS/DDoS Attacks, Worms & Port Scans
  - > – Precisely Define and Implement Network Security
  - > – Automatically Control P2P, IM and Spam Traffic
  - > FIND OUT NOW – FREE Vulnerability Assessment Toolkit
  - > <http://www.captusnetworks.com/ads/42.htm>

-----

> – \*\*\*\*\*

> SAVE PAPER – THINK BEFORE YOU PRINT!

> I ARBED PAPUR – PWYLLWCH CYN PRINTIO!

> \*\*\*\*\*

> \*\*\*\*\*

> SAVE PAPER – THINK BEFORE YOU PRINT!

> I ARBED PAPUR – PWYLLWCH CYN PRINTIO!

> \*\*\*\*\*

-----

> Captus Networks

SecurityFocus BASICS: Re: Re(2): Possible new virus?

- > *Are you prepared for the next Sobig & Blaster?*
- > – *Instantly Stop DoS/DDoS Attacks, Worms & Port Scans*
- > – *Precisely Define and Implement Network Security*
- > – *Automatically Control P2P, IM and Spam Traffic*
- > *FIND OUT NOW – FREE Vulnerability Assessment Toolkit*
- > <http://www.captusnetworks.com/ads/42.htm>

>-----  
>--  
>  
>  
>-----  
> *The information transmitted in this message is intended only for the person*  
> *or entity to whom it is addressed and may contain confidential and/or*  
> *privileged material. Any review, retransmission, dissemination or other*  
> *use of, or taking of any action in reliance upon this information by*  
> *persons or entities other than the intended recipient is prohibited. If*  
> *you received this in error, please contact the sender and destroy any*  
> *copies of this document.*

- >-----  
>  
>-----  
> *Captus Networks*
- > *Are you prepared for the next Sobig & Blaster?*
  - > – *Instantly Stop DoS/DDoS Attacks, Worms & Port Scans*
  - > – *Precisely Define and Implement Network Security*
  - > – *Automatically Control P2P, IM and Spam Traffic*
  - > *FIND OUT NOW – FREE Vulnerability Assessment Toolkit*
  - > <http://www.captusnetworks.com/ads/42.htm>

>-----  
>--  
---  
  
Sebastian Schneider  
straightLiners IT Consulting & Services  
Metzer Str. 12  
13595 Berlin  
Germany

Fon: +49-30-3510-6168  
Fax: +49-30-3510-6169  
www.straightliners.de

-----BEGIN PGP SIGNATURE-----  
Version: GnuPG v1.2.2 (GNU/Linux)

iD8DBQE/YN8sQ7mOWZBxbPcRAiX9AJ9cx dgX6tA1k04cI9cxNwUt72mt/QCgsMx2  
8MISJxxG1i8J53GAtyQHkxY=  
=e/AG  
-----END PGP SIGNATURE-----

Re: Re(2): Possible new virus?

Captus Networks

Are you prepared for the next Sobig & Blaster?

- Instantly Stop DoS/DDoS Attacks, Worms & Port Scans
- Precisely Define and Implement Network Security
- Automatically Control P2P, IM and Spam Traffic

FIND OUT NOW – FREE Vulnerability Assessment Toolkit

<http://www.captusnetworks.com/ads/42.htm>

---