

## Weird events: please advise

**Source:** <http://www.derkeiler.com/Newsgroups/comp.security.firewalls/2004-06/0598.html>

---

**From:** Writehand (*sophie.jameson\_at\_ntlworld.com*)

**Date:** 06/13/04

Date: Sun, 13 Jun 2004 22:01:53 +0100

Hi,

I would be seriously grateful if someone could take a look at this problem..

A close friend of mine has just taken a job with an IT security company. A condition of employment is that, unless agreed beforehand, all work (in or out of hours) becomes the intellectual property of his new employer. My friend has been working on some potentially valuable software with me and has no intention of handing it over to his new boss. He therefore made the required declaration and explained that this single project, nearly finished, must be agreed as separate from his new contract with them. Fine, they say. No problem.

Then, on the very first weekend after he started work, his home PC was hacked. He discovered his scheduler had been altered to run Windows update every five minutes – and this on his old home PC which runs Windows 98 and doesn't need an update. Weird stuff was happening.

He got off-line fast. A subsequent check found \*34\* different spyware programs on his PC. When he realised he was under attack he tried to delete the key files but could not do so online. He could only delete them after he'd pulled the plug on his broadband – i.e. someone else was already accessing them online.

I pointed out that coincidentally it is also only a week since he got broadband. I wonder whether his old virus settings/firewall were simply not good enough for a constant broadband connection with the extra risks it entails. So maybe that's the deal. After all, people who work in IT are often the worst at remembering to take precautions.

But he's very, very uncomfortable. Someone at work on Friday told him "You aren't nearly paranoid enough." Spooky, huh?

What does anyone out there think? Please answer soon, as he is extremely stressed about the situation and feels he may have to resign in the next 24 hours if he still feels so paranoid. Who wants to work with people who basically break into your house? An innocent "Duh"

comp.security.firewalls: Weird events: please advise

explanation is what I hope for – but any ideas would be very welcome.

Thank you,

Writehand