



The Day The Hard Drive Died

Disk security feature may be turned against you

Jürgen Pabel, CISSP

The German computer and technology magazine “c't” featured an article¹ about a Denial of Service (DoS) attack that most computer systems appear to be vulnerable to. These systems allow for hard drive passwords to be set via software (in contrast to only from within the computer's own configuration menu – the BIOS). While this may appear benign at first, it's actually quite significant: malware could set a secret password and thus lock the drive for anyone but the author of the malware. Although no such malware is known to exist, this is likely to change – the extortive potential is immense.

It's important to point out that this threat is not a universal one, it doesn't apply to computer systems using SCSI disks – significant numbers of servers are therefore inherently unaffected. However, ATA disks are becoming increasingly popular in server systems in addition to their ubiquitous presence in desktop and laptop systems. Laptops are also widely immune to the threat as this security feature was originally devised for laptops² and most models correctly restrict the setting of such a password to the BIOS. Desktop system manufacturers³ however seemed to have largely been indifferent about this and now most of us have to deal with it.

Corporate systems are an obvious target for such attacks, but the operating systems in corporate environments are at the same time the likeliest to be configured in a restricted manner. On a technical level this means, that most corporate users don't have administrative rights – without those, the operating system won't allow for the malware to communicate with the hard drive. However, if the potential malware attacks unpatched (or new) vulnerabilities, it could obtain administrative privileges and thus be successful in its attack.

It's only a password, can't it be cracked or circumvented? If we presume that the attacking party is competent enough to implement such a malware, what are the chances that they'll choose a weak password? As for circumventing it: yes, it's

1 Harald Bögeholz, “At Your Disservice”, c't 8/2005
<http://www.heise.de/ct/english/05/08/172/>

2 It provides laptop users with an easy and fairly effective option to protect their data in case of loss or theft

3 Actually, the BIOS manufacturers



possible, but you'll need professional data reconstruction specialists. While the costs for recovering a single disk drive are negligible for corporations, it's questionable if this still holds true when entire departments are affected. A good backup (and restoration) strategy may be a workable solution to this scenario, but naturally it's even better to prevent such an attack entirely.

System manufacturers are likely to provide BIOS updates fairly soon, but BIOS updates are often more complicated than usual software patches:

- some systems don't allow for the update to be applied from within the running operating system, thus making an automatic roll out highly complicated or even impossible
- every computer model has to receive its corresponding update, mistakingly running an update on an inappropriate model may actually cause harm to the system.

Fortunately, there's an easier solution: drives can be set into a special state that prevents future password activation attempts. However, this state has to be activated every time the system is started; c't magazine provides free downloads for Linux⁴, MacOS⁵ and Windows⁶ that activate this state. A BIOS update is still preferable, because it activates this state right after the system is turned on and therefore closes the small vulnerability window between powering the system on and the time the mentioned software is started.

Are you responsible for protecting your corporation's IT infrastructure? Then you better get into gear now. Problems of this magnitude are known to take a long time until deployment actually occurs. If you are worried about your personal computer, you should take a few minutes to download and install the provided software. While you're at it, make sure you're up to date on all security updates on your operating system and your applications – that's always good.

4 Linux Software (patched version of hdparm)
<http://www.heise.de/ct/ftp/projekte/atasecurity/files/hdparm-5.9-ct.zip>

5 MacOS (kernel module)
<http://www.heise.de/ct/ftp/projekte/atasecurity/files/atasecurity-mac.dmg>

6 Windows (installation as a system service preferable)
<http://www.heise.de/ct/ftp/projekte/atasecurity/files/atasecsvc10.zip>