

Forum: [Hack Forums](#)

Thread: [This gives me great scare](#)

Microrobot - March 3, 2013, 3:51 pm

<http://www.geek.com/articles/chips/300-tool-can-decrypt-gpg-truecrypt-files-without-a-password-20121221/>

How can we prevent this tool from working?

you are a skid - March 3, 2013, 4:08 pm

prevent it by using a decent "encryption tool".

MajorFail - March 3, 2013, 4:56 pm

Disable firewire in BIOS and powerdown your system (do not use hibernation) if your not using it. If anyone gets their hands on your PC while it's booted up and the key is still in memory (ie. you mounted the encrypted volume) they can extract the key. Even a few minutes after shutting down your PC the key can still be extracted (see ' cold boot attack').

RyanC - March 3, 2013, 4:57 pm

Isn't this like multiple years old?

Cody8295 - March 3, 2013, 5:06 pm

They mention in the article that this works by pulling the public key from your RAM. Therefor you should be safe if you restart your computer after using TrueCrypt. That orrr... Find a way to "blank" certain parts of your RAM?

MajorFail - March 3, 2013, 5:07 pm

(Mar 3, 2013 05:57 PM)Who? Wrote: [\[CITE\]](#) Isn't this like multiple years old?

Yes, at least 2008 so it's pretty old news.