

15 September 2007

By: Alexandru Dumitru, Security News Editor

## [Security Brief: Hack Week](#)

*10 to 14 September*

**Hackers**  
  
**Hackers**

I chose to call this the 'hack week', not because we had any great hacks or anything spectacular, but because we learned a lot about hacking. And by this, I mean lots and lots of things, fancy hack methods, as well as some "hulkish" ones. We had news about hackers stealing passwords, about exploits and certainly, hack aftermath. Knowing that malicious users have a lot of power is not something that I would call great news. But the fact that we know their methods and study them just makes us stronger in the fight. By knowing what they can do against us, we can defend ourselves better. Here's some stuff about hacker tactics and how they work: Many of you probably ask themselves how come so many hack attacks occur daily and where all these skilled black-hatters come from. Well, the thing is that hackers aren't really as skilled as they may seem, it's just that a lot of users are either unfamiliar with the basics of security or simply don't give a damn about it, but I've learned that 40% of the Europeans suffer from digital illiteracy. Forty percent! That's huge! No [wonder](#) we get hacked... This week, two new scam types popped up as well as one interesting spam message. The two scam were: cybersquatting and e-mail-phone scam. None is really something new, but they've made the news because their numbers seem to have increased as of late. Then, there was that [stupid](#) spam I got regarding the Yahoo! Messenger closing down. This is another thing that proves people get hacked because they're too naïve. The spam message contained info regarding the closing of the free YM and a link that you should click in order to save your account. Of course, it was a virus. That was a good example of social engineering based hack! One of my favorite hacks of the week was the one against the Great Firewall of China. I had an [article](#) about it on Thursday. Thing is, you can bypass their filters using spammified words. Yeah, that's right - their GFC block sites that contain certain words, but if you spell them like spammers do, I mean "mas\$acre" instead of "massacre" then the filter will dub your website as "clean". Then, on Wednesday, there was another interesting [article](#) about corporate network security. It was actually more about how to avoid hacks than about how black hatters work. But in any case, the basic idea was that most of the data leaks are caused by the employees' sloppiness rather than by a skilled hacker's work. On Tuesday, there was that thing about how white-hatter Dan Egerstad managed to use Tor in his advantage, to get thousands of e-mail credentials. He's a pretty smart guy and fortunately, he only did it to [show](#) companies and governments how insecure their systems actually are and to make them take security more seriously. This is a pretty good measure, if you ask me, since a lot of folks only act against a threat after they've been hit. And my absolute favorite piece of news on hacks was on Friday. I don't know how I do it, but I always seem to get to the best news on Friday. In any case, I wrote [two articles](#) about how competition could sabotage you over the Internet and how to dodge those threats. The first piece was all about the simpler ways of doing this, while the second regarded complex methods. It's a good thing to battle competition, but resorting to hacking is really bad, mostly because it's illegal, and then, it's unethical as well. So that was about it, regarding hacks this week. Well, we also had some good news, as I found out that Storm is finally being tackled by ThreatStop. Also, I've learned that the StopBadware researchers are really doing a good job against web-based threats. Those and the fact that some hackers have been busted were the encouraging news, but as far as Storm goes, it's not yet stopped. As I've said on Monday, this virus kind of reminds me of Skynet in the Terminator movie. For one thing, it formed a botnet of huge power, controlling millions of computers, but that's not what makes it resemble the famous Skynet. As you might remember from the movie, everything that

opposed the virus was taken down; well, the botnet has recently launched some attacks against spam-fighting websites. Fortunately, it is nowhere near the stuff we see in the movies, as it is not self-conscious, and I don't think that it will ever be. And here is this week's piece of advice: If you want to properly enforce security, it doesn't hurt to be a little bit paranoid. Also, when thinking about how secure you are, try and look at things from a hacker's perspective. Don't go like "Oh, I did this and I did that - I'm secure now!". I would advise you to think about such possible scenarios: "Now, if I were a hacker, what would I do to this network?" And when you've considered your vulnerabilities, try and patch them up!