FirstRand

Hackers and Hacking

Author: Peter Dearlove

Why is something so apparently mindless and nasty now rampant? Are hackers just thieves looking for an open window? What is to be done to solve the biggest threat to our sophisticated existence?

Hacking, hackers, white hats, black ones, and grey.

There are perhaps, nine, ten, eleven, twelve, thirt... different kinds of computer virus, and the number is growing almost as fast as you can say the number is growing too fast. Then again, there are nine, ten, eleven thousand hackers creating new ones and using them to do one, two, three, four or fi... different criminal things.

It is not an easy business to keep your finger on, to fight, to write books about, or to try to control. It is, according to people who track these things, the most important issue and the biggest threat of our times, apart that is, from climate change and maybe the exploding population.

When man-made computer infections first came to general attention and were likened to a virus they seemed more naughty than threatening. For reasons now hard to pin down, wayward young computer programmers, widely assumed to be teenagers, took delight in making people's computers disobey instructions and do weird things. This they learned they could by inserting a string of rubbish instructions into the normal instruction parade that made your computer do the job you wanted from it – writing letters, accounting your cash, balancing the books and adding up long columns of enormous numbers. At worst, in those long-gone halcyon days of Green Screen clubs and a nerdy devotion to fiddling with keyboards, your computer might suddenly stop, pull faces at you and shut down without permission. And sometimes just give up the ghost completely.

It was not easy to make any kind of sense of this phenomenon but we were not left to ponder the motivation for long. The day soon came when money turned out to be behind it all. Using any one of a growing number of viruses to gain access to your computer, thieves found out that the process would also give them access to a veritable store house of private information and your personal store of money. Moving your cash into their pockets became alluringly simple.

Theft is what hacking is still mainly all about, though much bigger, more varied, vastly more complex and sophisticated, and frighteningly dangerous. In a comparatively short time it has progressed from teenage mischief into a multi-million dollar business, spawning an entire sub-culture with its own curious terminology. By their own definition hackers are now black hats, white hats, or grey. The bad ones are black, the good ones white and those in between are grey. Black hats pose the threat, white ones are the defenders, and grey hats are a bit like mercenaries, ready to work either way to make a living Hacking, it must be said, is not in itself a cyber crime although it can be an aspect of it and is often simply bundled in with it for statistical and other data building reasons. Cyber crime covers many other unpleasant activities including various forms of computer fraud, blackmail, paedophilia and pornography, all of which are growing at headlong pace.

But it is out of hacking that has come the distinctly sinister concept of cyber warfare. It should have been no surprise that the fundamentals of computer crime would be dragged in to battles between nations, and yet it did seem to catch people off guard when one country was accused of interfering with another's elections via computer science and the massive loophole that the internet provides. If you create a regiment of competent hackers and give them all the latest computers plus internet access, there is simply no telling what military mischief they could get up to: derailing plans, sabotaging systems and destroying defences.

So now the race is on everywhere to try to plug the holes, and there are good premiums available for people with the skills and the interest to work on the cyber front line. Strange to relate, among front-line fighters are several children under the age of 10. When day-to-day computer circumstances revealed their talents their parents had the wit to bring them to the notice of the white hat brigade, and now they are all working on the white side. One of them who is 11, pulled off his first hack when he was 5.

Aside from this kind of precocity, hacking your way into a locked and cryptically sealed computer depends more on patience and perseverance than raw whiz-kid talent. Much time is involved in searching for and finding passwords or creating a way around them.

What is to be done about it? Should hacking and its many criminal offshoots be worrying us all? Or does it matter only to those with the most to lose?

Turning for guidance to people in the business is instructive.

Based on a recent worldwide survey of IT professionals it is clearly a problem for us all. Three quarters of the men and women surveyed said they were personally worried about cyber crime and cyber warfare and could see no quick solution to any of it.

They worried most about the warfare threat of course and in particular the chance that they and their businesses could become victims of collateral damage if things get really hot. But they were also deeply concerned by the growth and spread of hacking for its disruption of business. The potential for utter internet and computer network chaos is real and alarming, and at present the struggle is tilted in favour of the criminals because the initiative is always with them. Solving new threats means identifying them, and while there are now dozens, perhaps hundreds, of companies and products working day and night to provide internet security, there is little co-operation of the sort you would expect in a case of dire emergency. Which is why one longer-term solution being canvassed may offer a glimmer of hope of turning the tables.

A handful of influential people have proposed the world's first truly non-political, truly international, wholly scientific establishment – call it a university if you like, or better still an institute, where smart computer brains can study and teach one subject only – making computer security absolutely break-proof. They point to the way Britain attacked the German 'Enigma' coding problem at Bletchley Park in World War 2 when the nation's brightest mathematicians were massed together tor solve a single problem. It is a compelling notion, one that all nations would surely wish to be part of – if only to prove their sincerity when pressed to deny their part in any mischief.