BIZCOMMUNITY

# Hackers pose threat to Africa's governments

Hackers have claimed the scalp of the South African Ministry of State Security's Twitter account, underlining concerns that Africa may be the soft underbelly of global cyber security.

As part of what was described as a large-scale attack spammers hijacked the @StateSecurityRS account to advertise a "miracle diet" before officials were able to change the password and regain control.

"Necessary security measures have been put in place to avert similar occurrences," State Security spokesman Brian Dube told *AFP*.

While many South African users of the social media network reacted with amusement, cyber security officials fear the next high profile attack on an African government will not be so harmless.

"It wouldn't be hard to shut down the government. There's very little in place, so even the most basic of attacks, in most cases, get through," said Craig Rosewarne, founder of the South African based consulting firm Wolfpack Information Risk.

With funding from the British government, Rosewarne's consulting group recently published a much-heralded threat analysis on the continent. According to the report, most developing African nations have been either unwilling or unable to secure their rapidly expanding online networks and infrastructures.

South Africa is a particular source of frustration. Rosewarne's analysis found that corruption is driving a proliferation of digital crimes throughout the country.

"We've delayed so much that other African countries have actually overtaken us," he told *AFP*.

Over the past few years, hundreds of criminal syndicates have taken advantage of lax cyber security to launch relatively unsophisticated attacks, often using government or business insiders to exploit vulnerable networks.

It is estimated that cyber crimes resulted in R2.65bn in damages and losses across South Africa in 2011, the last year that reliable figures were published.

"While we're seeing a huge surge in financially motivated crimes, we're also seeing an upswing in hacktivism," Rosewarne said. "And that's where you'll get the scary guys - the guys that will go full out to make it happen."

## Team GhostShell


The most ambitious of these homegrown hacking collectives is Team GhostShell. Last year during its Project White Fox campaign, the group published 1.4m hacked government and corporate documents from overseas institutions.

In October, the prolific hacker group Anonymous publicly distanced itself from GhostShell after the latter leaked the email addresses, passwords and identifications of 120,000 students from more than 100 universities worldwide.

With ANC leaders laying out a June deadline for adoption of the proposed *Secrecy Law*, digital security experts worry the next few months could bring an onslaught of cyber attacks from GhostShell and its allies.

"The moment the proposed Secrecy Law is enacted, it's going to be a trigger to stir up and bring these collective partnerships together," said Rosewarne.

The African Union and the UN Economic Commission for Africa believe these hackers, along with their financially motivated counterparts, pose a dire threat to the continent's growth plan. To help national governments combat this insurgency, they drafted a regional convention on cyber legislation that is adoption from member countries.

"Without such protection, countries cannot take advantage of the digital economy in a sustainable way," said Aida Opoku-Mensah, director of UNECA. "Consequently, the convention sends a strong political message that Africa is ready for the knowledge economy."

Even much-maligned South Africa is beginning to step up its efforts to thwart online crimes. The country's director of cyber security announced that final plans for a national hub to combat online threats will be unveiled in July.

Meanwhile, a cohort of cyber inspectors are being trained to ferret out criminals - the first national efforts to train specialist law enforcement personnel since 2003.

"We've got capability, but it's fragmented," Rosewarne said. "We need a senior person to take the lead on this and to actually put in the necessary resources and look at the bigger picture and get things going in this country."

This lack of leadership has left local police dangerously ignorant of cyber security laws and the government still has not implemented critical response teams that can respond to attacks. Until all the pieces come together - Rosewarne believes this could take two years if fully prioritised - then South Africa, like most of the continent, will continue to lag behind other mature economies that have already constructed robust digital defences.

Source: *AFP* via I-Net Bridge