South Africa has crossed the cyber Rubicon

Johannesburg 14 July 2016 – The recent spate of well-publicised cyber-attacks on South African organisations should be a wake-up call to government and corporates indicating that the country is amongst those being targeted globally, says Evert Smith, Threat Intelligence Lead at Deloitte South Africa.

“South Africa is no longer isolated when it comes to hacktivism and other cyber-related attacks. Some of the most notorious international groups have made their intensions clear by focusing on several high-profile organisations,” he says.

“As part of the Deloitte Threat Intelligence monitoring, we see how Africa is targeted by a variety of threat actors with statistics from security vendors supporting what we see on our monitors.”

While much focus has been placed on Web site defacement, attacks will typically not stop at that. Accessing sensitive back-end data and sharing it with the rest of the world to drive a political (or other) agenda is a fundamental part of the malicious user’s agenda.

“What is more, compromising a parent company or a large group could result in a cascading effect where affiliated pariah companies are identified. This will see even more attacks taking place, further putting financial and reputational pressure on those entities.”

A recent database leak highlighted the association between the compromised organisation and high profile and controversial suppliers. This might result in activists now starting to focus more on the company due to its relationship with these suppliers.

Smith believes that companies can ill afford to put their heads in the sand and think it will not happen to them. The evidence is now very much in the public domain.

“Based on local and international research, it is evident that the recent attacks will just be the start with even more public ones coming in the near

future. There might be a perception that hacktivists do not have the skills to pursue a concerted agenda against a country or industry. Yet, this could not be further from the truth."

He says that the likes of Anonymous, although not always as organised as they could be, are dedicated in what they do and once they have identified an organisation, it is highly unlikely for it to leave unscathed.

"Decision-makers often underestimate the seriousness of these attacks and the impact it could have on the economy of a country. And the more controversial your organisation and the people working there, the more likely it is that you will have the spotlight on you."

Take for example Operation Icarus. Announced by Anonymous in May, the hacking collective threated several financial institutions as part of a month-long assault. As part of their campaign manifesto, several prominent South African entities were included in the published target list, and the evidence is there that these targets were probed. Even though these attacks are specific to finance, other industries and organisations are just as likely to be attacked.

"Many of these could become collateral damage as a result of such a focused attack. There is also nothing stopping this and other hacktivist groups on targeting the critical infrastructure of the country. Private and public sector entities need to re-evaluate their cyber-security and adopt both defensive and offensive measures to protect themselves wherever possible."