KEMPTON EXPRESS

Weak spots in anti-poaching technology an easy target for hackers

A recent study suggests regular software updates, firewalls and intruder detection systems among the options to guard against cyber-attacks threats.

2 hours ago

Content Supplied 2 minutes read

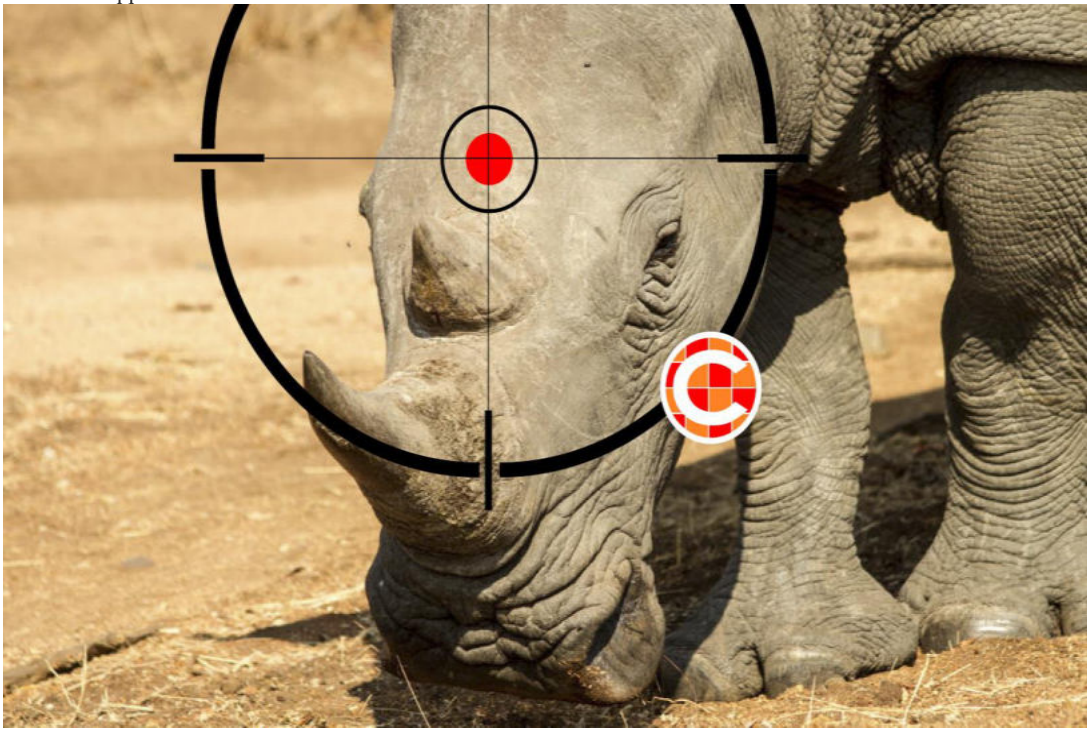


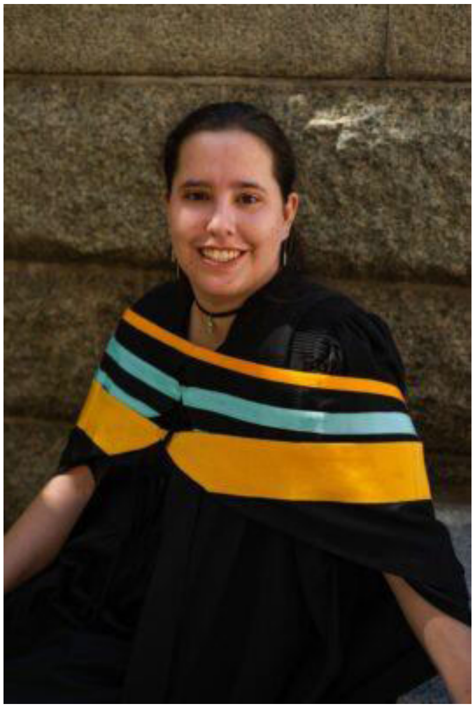
Photo used for illustration purpose only.

During a time in which South Africa’s wildlife is under attack by poaching, a new study has shown that popular anti-poaching technologies could be an easy target for cyber-attacks.

Stellenbosch University student Christelle Steyn, who is part of the Orange Cyberdefence Academy, conducted research that shows that various technologies, such as tracking tags, CCTV, mobile apps and drones could increase the risks of cyber-attacks.

Steyn’s research established that communication networks and IT infrastructure must be well set up and securely authenticated for greater protection of information, anti-poaching units and, ultimately, animals.

Steyn, who is a certified field guide, made these findings in her thesis T*owards a Critical Review of Cybersecurity Risks in Anti-Poaching Systems in South Africa*.
As part of her study, Steyn used a network software emulator to simulate a hypothetical network of anti-poaching technologies that could be used in the conservation of wildlife species such as rhinos, elephants, pangolins and lions.



Christelle Steyn from Orange Cyberdefense Academy. Photo: Supplied.

She points out that anti-poaching operations do not want to reveal real world data about the status and capabilities of their systems or their mitigation strategies.

Steyn used the simulation to run various cyberattacks identified as pertinent to show the risks of such a network. Using the data from the simulation, she was able to perform threat modelling to determine the severity of potential threats to anti-poaching networks. These attacks were then mitigated through system configurations.

Steyn says that due to the nature of their simulation, many of the attacks targeted the backbone of the network – the router and switch.

"These network appliances were found to be the most vulnerable to the broad classes of Denial of Service (Dos) and Man in the Middle (MitM) attacks. DoS attacks disrupt a service, while MitM attacks intercept data on the network.

"Through my simulation, I discovered that many security features are not always applied by default when acquiring a new network appliance such as a router or switch. So, from the start, correct and adequate configuration is necessary.

"Since many of the technologies used in anti-poaching operations are connected to either another device, a database, a network, or the Internet to transmit data, they are all vulnerable to attack. The systems used to store the collected data are ultimately at most risk, especially if they can be accessed by cybersecurity compromises of the network or connected devices."

Steyn points out that as soon as the real-time data needed for anti-poaching operations is transmitted over a network, there is the possibility of an attack. She adds that common attacks on anti-poaching networks are likely to be aimed at intercepting or retrieving data, or disrupting the network to block monitoring or delay response.

According to Steyn, not all networks are adequately protected and those that are could still be subject to very sophisticated and cutting-edge attacks.

“While a typical poaching recruit in the field might have little technical know-how and give the Joint Operations Centre and rangers a wide berth, the syndicates funding them may be able to provide the skills, training, and equipment necessary for someone to gain access to the anti-poaching systems and communications of an area or park.

“Anti-poaching efforts are implemented by governments, non-profit organisations and private entities, with varying degrees of skills and financial resources.”

Steyn recommends a comprehensive anti-virus programme and regular software updates, Intruder Detection Systems and firewalls, an extra layer of protection beyond a username and password, regular security audits by an expert, and creating a security-aware culture among staff to mitigate some attacks and secure the network overall.

She says her study creates awareness of cyber threats and provides mechanisms that can be used to mitigate them.