African banks targeted by notorious hacking group

Kaspersky security researchers have reported on thousands of notifications of attacks on major banks located in sub-Saharan Africa. The malware used in the attacks indicates that the actors are most likely to belong to the infamous Silence hacking group, responsible for the theft of millions of dollars from banks across the world. A report on the **iAfrica** site notes that the typical scenario of the attack begins with a social engineering scheme through a phishing e-mail that contains malware to a bank employee. From there the malware gets inside the banks' security perimeter and lays low for a while, gathering information on the organisation by capturing screenshots and making video recordings of the day to day activity of the infected device. Once attackers are ready to take action, they activate all capabilities of the malware and cash out using ATMs and other equipment. The attacks are ongoing and persist in targeting large banks in several sub-Saharan Africa countries. 'They live up to their name. **Their operations require an extensive period of silent monitoring, with rapid and coordinated thefts.** We noticed a growing interest of this actor group in banking organisations in 2017 and since that time the group would constantly develop, expanding to new regions and updating their social engineering scheme,' said Sergey Golovanov, security researcher at Kaspersky.