BIZCOMMUNITY

Malware attacks in Africa reach 85 million in 6 months

According to research done by Kasp, malware is rife across Africa with various countries exhibiting strong growth in all malware types in the first half of 2021 when compared to the same period last year. This is a 5% increase in the region, as cybercriminals and hackers continue to focus on African countries considering digital transformation advancements and the increase in remote working resulting from the Covid-19 pandemic.

Source: ©rawpixel – 123RF.com

Overall, four countries account for 85 million attacks, with South Africa being the most targeted - 32 million attacks, followed by Kenya (28.3 million), Nigeria (16.7 million) and Ethiopia (8 million). All countries but Kenya saw the relative growth of all malware attacks. Ethiopia and Nigeria have seen an increase of 20% and 23% respectively and South Africa an increase of 14%, while Kenya's number of attacks decreased by 13%.

Even though the scourge of malware has always been of concern, the past 12-months have highlighted how hackers are refocusing their efforts to compromise consumer and corporate systems and gain access to critical data and information. Given the growth of digital transformation across Africa since last year, the continent has become an attractive target for those looking to exploit a lack of user education and cybersecurity understanding. This has contributed to a large number of personal devices still not having any form of cybersecurity software installed," says Bethwel Opil, enterprise sales manager at Kaspersky in Africa.

"Malware can get onto a device in several ways. For example, clicking on an infected link or advert, opening an attachment in a spam email, or downloading a compromised app. This means proactive malware protection is essential to safeguard individual users and corporates against these threats," adds Opil.

There are several best practices to consider when it comes to malware protection. Kaspersky recommends the following:

- Install anti-virus software on every device that connects to the internet.
- Only download applications from trusted sites. Even then, always check the app permissions and, if certain things do not make sense, do not install the programme.
- Never click on unverified links, especially when coming from suspected spam emails, messages, or suspicious-looking websites.
- Keeping operation systems and applications always updated with the latest patches.
- Be wary of using free Wi-Fi at coffee shops, restaurants, and other places as hackers can snoop for unprotected devices.