Rwanda is among African nations experiencing higher risk malware attacks on the continent compared to Ghana, South African, Zambia and Uganda.

Latest Data from cyber security firm Kaspersky shows that Rwanda at 46 per cent is ranked 4th.

For countries monitored on the African continent, the three countries which experienced the most attacks on ICS infrastructure were Ethiopia (62%), Algeria (59%), and Burundi (57%).

Further, Kenya is at 41 %, Nigeria and Zimbabwe both at 40 %, Ghana at 39 %, Zambia at 38 %, and South Africa and Uganda both at 36 %.

Throughout 2022, 40% of industrial control system (ICS) computers globally and 47% of ICS computers in Africa were attacked with malware, the report says.

In addition, the report explains that a high threat landscape on the continent affected both public and private sector entities, especially those in critical sectors like energy and noted that despite all the innovations in modern cyber security solutions, human error still play a significant role in compromising Industrial Control Systems (ICS).

An ICS can be considered as a collection of personnel, hardware and software that can affect or influence the safe, secure and reliable operation of an industrial process. Information technology is one component of this environment with operational technology (OT) another key element, Kaspersky ICS CERT said.

Kaspersky Middle East and African region technology expert and consultant Brandon Muller says that human error still plays a significant role in compromising ICS systems. As such, it needs to be managed much more proactively. This requires utility companies, mines and other companies operating in the industrial environment to look at building a Human Firewall.

One of the best ways to achieve this is through the right security awareness and training solutions that deliver training that is easily digestible, practical and memorable, so that it will always stay top of mind, he notes.

“ICS malware attacks are a high-growth threat landscape in Africa. Companies must provide training to ensure staff is armed with the very latest skills and knowledge, especially given how quickly cyber incidents evolve,” adds Muller.

“Effective OT cyber security measures must, therefore, include industrial endpoint protection to prevent accidental infections and make motivated intrusion more difficult, OT network monitoring and anomaly detection to identify malicious actions on the level of programmable logic controllers, and dedicated expert services to investigate the infrastructure, conduct expert analytics, or mitigate the impact of an incident,” the team advises.

In 2018, Rwanda passed a cyber-crime law aimed at helping the government and the private sector to combat cyber crime.

The law targets to safeguard private and government information and infrastructure against online crimes and cyber-attacks.