

A group of hackers, allegedly associated with China, conducts a large -scale cyberspion campaign aimed at vulnerable virtual systems VMware ESXI and VCENTER.

Since the beginning of 2025, specialists from Sygnia have been investigating a series of attacks united under the name Fire Ant. Attackers gained access to internal systems of organizations through the vulnerability of CVE-2023–34 048 in the VMware Vcenter, which has been known for almost two years.

Of particular concern is that hackers were able to penetrate into the isolated parts of corporate networks – those that are usually protected from external access. They used complex and secretive methods to get around the network segmentation and gain access to closed data.

Experts urge the companies to urgently check and update their VMware virtual environments.