In March 2021, BAE Systems began investigating a campaign utilising a 0-day exploit in Pulse Secure VPN appliances, which led to the identification of a wide spread campaign affecting over 40 high-profile US companies and government organisations.

Key operational mistakes made by the group led to the tracking and discovery of backdoors in the networks of over 40 organisations.

After subsequent public reporting by FireEye in April, we observed an immediate clean-up of most backdoors. However, this was rushed and incomplete, leaving backdoors behind in a handful of networks.

Appliances such as VPNs are blind spots for network defenders. Attackers have caught on to this and organisations need to pay more attention to how they monitor for, and respond to, these types of intrusions.