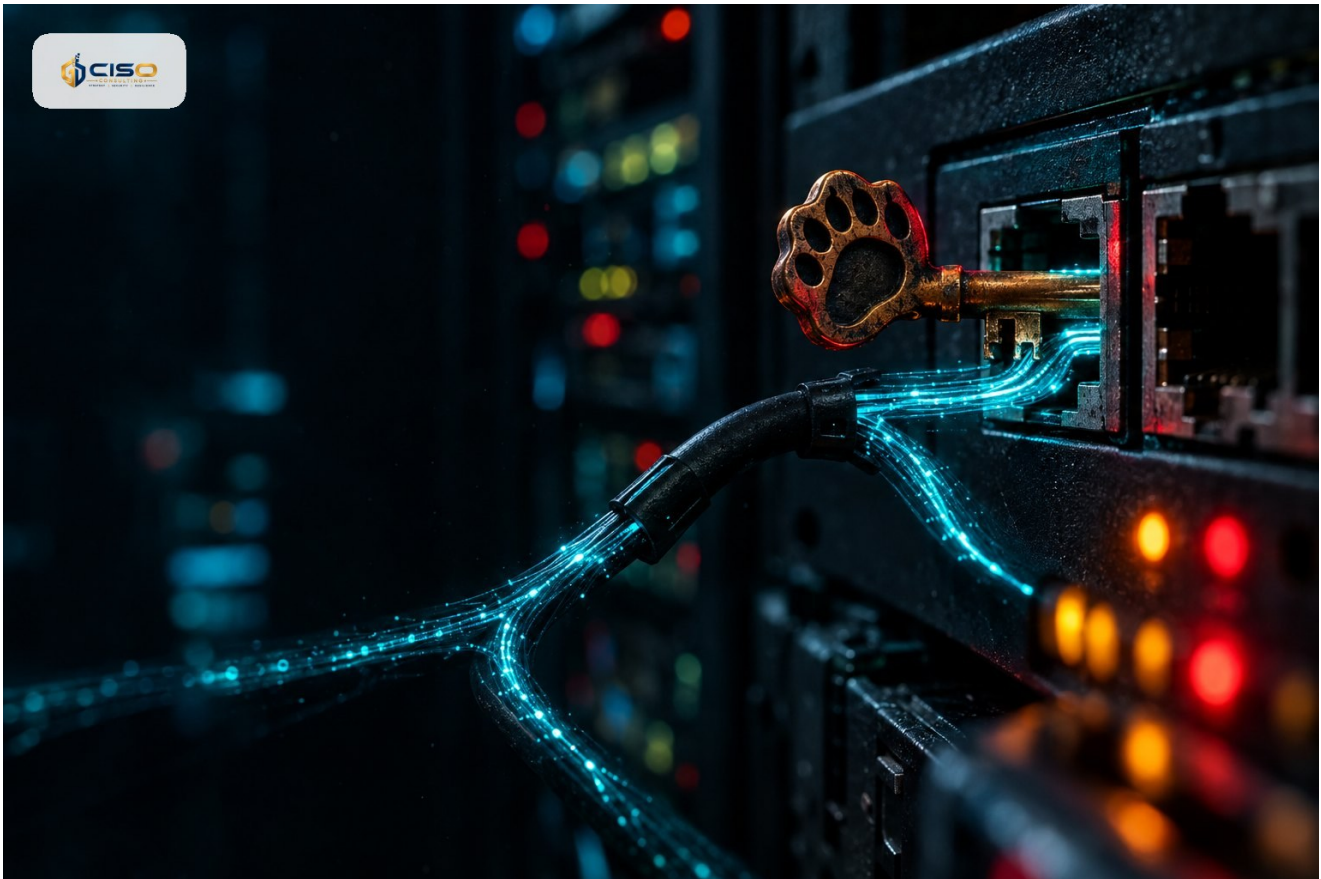


NCSC: APT28 hijacks vulnerable routers to redirect traffic and steal credentials



The UK NCSC advisory says Russian group APT28 exploited vulnerable routers for DNS hijacking, intercepting traffic and harvesting passwords and access tokens. It urges securing management interfaces, patching and two-step verification.

- APT28 exploited vulnerable routers to carry out DNS hijacking and reroute users' traffic through attacker-controlled servers.
- The goal was to intercept traffic and harvest passwords and access tokens from personal web and email services.
- The activity is assessed as likely opportunistic, casting a wide net before narrowing to targets of intelligence interest.
- The UK has previously linked APT28 to Russia's GRU, Military Unit 26165.

- Recommended mitigations: protect management interfaces, keep devices and software up to date, and enable two-step verification.

The UK National Cyber Security Centre (NCSC), part of GCHQ, has published an advisory describing how the Russian state-linked group APT28 compromised widely used routers. The access let the group quietly send users' internet traffic through malicious servers it controlled.

What the advisory describes

The actors used vulnerable routers to support DNS hijacking. DNS is the service that lets people reach websites by name rather than by IP address. By interfering with it, attackers can send users to malicious sites built to capture login details. According to the advisory, this allowed interception of traffic and collection of credentials, including passwords and access tokens, from personal web and email services.

The NCSC assesses the activity as likely opportunistic. The actor reaches many potential victims first and then focuses on those of intelligence interest as the operation develops. The UK has previously attributed APT28 to Russia's GRU 85th Main Special Service Centre, Military Unit 26165. The group is also known as Fancy Bear, Forest Blizzard, the Sednit Gang and Sofacy.

Why it matters for regulated institutions

The advisory is a reminder that edge devices such as routers are a route to credential theft, including from staff using home or small-office networks. The source does not mention activity in Saudi Arabia, but the techniques apply to any organisation relying on similar devices.

The NCSC's mitigation advice centres on protecting the management interfaces of systems, keeping devices and software maintained and up to date, and setting up two-step verification. Network defenders are encouraged to read the full advisory and apply its guidance.

What to do now

1. Inventory routers and other edge devices in use, including branch and remote-work equipment, and confirm their firmware is current.
2. Restrict management interfaces so they are not exposed to the internet and are reachable only from trusted administration networks.
3. Review DNS settings on edge devices for unexpected resolvers or changes, and monitor DNS configuration for drift.
4. Enforce two-step verification on email, web and remote-access services so stolen passwords alone are not enough.
5. Brief the security team on the techniques in the NCSC advisory and add DNS hijacking to detection and incident-response scenarios.