Joint advisory exposes China-linked Integrity Tech's role in global network compromise



The UK NCSC and partners from six countries issued an advisory on Integrity Technology Group, which they say enabled China-linked actors to compromise networks worldwide using AI-assisted scanning, botnets and manual exploitation.

- The advisory is co-sealed by the NCSC and agencies from Australia, Canada, Japan, New Zealand, Spain and the United States.
- Integrity Tech, a China-based company with reported government links, is said to support actors who develop and sell tools, acquire and host infrastructure and compromise networks.
- The activity combines AI tools such as automated scanning, large-scale botnets and hands-on exploitation to steal confidential data, including in critical sectors.
- The activity is consistent with campaigns also known as Flax Typhoon, Ethereal Panda and Red

Juliett.

- The NCSC urges all organisations to understand the techniques used and follow the advisory's mitigation advice.

The UK National Cyber Security Centre (NCSC), part of GCHQ, has published a joint advisory with eight international partners from six countries. It describes how Integrity Technology Group (Integrity Tech), a China-based company with links to the Chinese Government, has enabled China-linked cyber actors to exploit and compromise networks belonging to organisations around the world.

What the advisory says

According to the NCSC, the actors combine AI tools, such as automated scanning, with large-scale botnets and manual exploitation techniques. Their aim is to compromise networks and steal confidential data, including from critical sectors. The advisory also says the company employs people who support wider malicious activity: developing tools for use and sale, acquiring and hosting infrastructure, and compromising networks.

The reported activity is consistent with campaigns publicly known as Flax Typhoon, Ethereal Panda and Red Juliett, among others. In September 2024, the NCSC and partners had already identified Integrity Tech as the operator of a substantial botnet used by Flax Typhoon. The UK government sanctioned the company last year.

Why it matters

The NCSC stresses that the breadth of targeted sectors shows the scale of the threat, and that all organisations should read the warning and engage with its guidance. The advisory is co-sealed by agencies from Australia, Canada, Japan, New Zealand, Spain and the United States, and is available on the FBI website.

The source does not name specific victims or vulnerabilities. Security teams should therefore treat the advisory's own mitigation guidance as the primary reference and compare it with their current controls.

What to do now

1. Obtain the joint advisory from the FBI site and have your security team map its mitigation advice against current controls.
2. Check whether threat intelligence feeds and detection rules cover the campaigns named Flax Typhoon, Ethereal Panda and Red Juliett.
3. Review exposure of internet-facing systems and devices, given the use of automated scanning and botnets.
4. Consider proactive threat hunting to find gaps that routine monitoring may miss.
5. Brief senior management and, where relevant, report through your NCA and sector regulator channels in line with your incident procedures.