FOR IMMEDIATE RELEASE

UK Businesses Face "Permanent" Cyber Pressure as Attackers Refine Tactics in Q1 2026

HASTINGS, UK – New data released today reveals that UK businesses are operating under a sustained level of cyber threat, with high-volume automated probing now a permanent fixture of the nation's digital landscape.

The Q1 2026 Cyber Threat Analysis from Beaming shows that while attack volumes have plateaued since the record highs of late 2025, the intensity of activity remains significantly elevated compared to historical norms.

Consistent Pressure and Shifting Tactics
Between January and March 2026, UK companies were targeted by an average of 1,988 cyberattacks every day. Although this is a minor 2% decrease from the previous quarter, it remains almost identical to the high levels of activity recorded during the same period last year.

While the number of attacks held steady, the underlying infrastructure used by criminals has shifted. The number of unique IP addresses used to launch attacks fell by 14.6% this quarter. This suggests that attackers are using a smaller, more concentrated pool of devices more intensively to conduct their campaigns.

Web Applications Under Fire
The report highlights a concerning trend: a marked increase in attempts to breach web-based services. As more businesses move core operations and customer interactions to the cloud, attackers are refining their methods to target public-facing websites and online portals.

Remote control applications and file-sharing services also remain primary targets, as they offer a direct gateway into internal networks for those without robust security measures.

Geopolitical Influence
The geographical origin of these attacks continues to mirror global events. In the first quarter of 2026, China and the USA remained the most common locations for attacking IP addresses. Experts warn that shifts in international relations frequently dictate the focus and origin of digital hostility.

Sonia Blizzard, Managing Director of Beaming, commented:

"Security is no longer a 'one and done' task; it is a fundamental part of running a modern business. The best way to stay ahead of evolving tactics is to embed security into your everyday culture. Working with a specialist partner can provide the expertise needed to turn that constant pressure into a manageable, proactive defence."

Guidance for UK Business Leaders
In response to these findings, Beaming recommends four critical steps for businesses to protect their operations:

Secure Remote Access: Ensure all remote tools are protected by multi-factor authentication (MFA) and are only accessible via a secure VPN.

Prioritise Patching: Neutralise automated "noise" attacks by maintaining a strict patching schedule. The Cyber Essentials update in April 2026 requires patching within 14 days of release.

Monitor Global Trends: Stay informed through threat intelligence feeds to anticipate changes in threat types linked to international politics.

Bridge the "Human Gap": Conduct regular staff briefings on phishing and social engineering to ensure employees remain a strong line of defence.

ENDS

For more information please contact:
Rachael White | Marketing Manager | Beaming
E: marketing@beaming.biz

Notes to editors

- Beaming has analysed cyberattacks in real-time targeting thousands of UK-based businesses since the beginning of 2016 to better understand their nature and origin.
- To download charts to accompany this press release and a picture of Sonia Blizzard please visit **https://www.beaming.co.uk/media-resources/**

About Beaming: www.beaming.co.uk Established in 2004, with offices in Kent and Sussex, Beaming is a specialist internet service provider (ISP) for businesses, supplying thousands of organisations across the UK with fast, reliable, and secure connectivity, voice and managed services.