CaptiveCrunch: the hotel Wi-Fi as a collection point

A Russian state cluster takes control of hotel Wi-Fi, forges what the network tells a guest's laptop, and serves a fake update. The target is the traveller, not the hotel.

INCIDENT DETAILS · 5WH

Who Actor - Storm-2945, held by Microsoft to be a sub-cluster of Midnight Blizzard (APT29), which the NCSC holds to be almost certainly part of Russia's SVR.
What A traveller-targeting campaign, CaptiveCrunch. Compromised hospitality Wi-Fi delivers a Go-based Windows RAT, CornFlake, plus token theft.
Where Hospitality networks with captive portals, worldwide. Established targeting: government, diplomatic, NGO and IT, in the US and Europe.
When Traffic manipulation observed since early May 2026; Microsoft published 31 Jul 2026.
Why Access to the accounts of corporate and official travellers, supporting SVR collection.
How The captive portal gateway was also the DNS resolver. Control of it let the attackers forge DNS answers and redirect a connectivity check to a fake update.

IMPACT

- Individual: a traveller's laptop compromised on arrival, through an action the job requires.
- Institutional: stolen session tokens and device-code abuse reach the corporate and diplomatic accounts behind the device.
- Remediation: token theft does not respond to a password change - the same structural problem as the Exchange OWA campaign.
- Sector: hospitality networks are now an exploited link between an organisation and its own people.

SEQUENCE OF EVENTS

A Apr 2026: Microsoft discloses the separate Forest Blizzard router hijacking
B 23 Jul 2026: ReliaQuest reports doppelganger domains abusing the Entra ID device-code flow
C 31 Jul 2026: Microsoft publishes the CaptiveCrunch campaign in full

1 Guest joins the hotel Wi-Fi; the gateway is also the DNS resolver
2 Forged DNS answers redirect the laptop's connectivity check
3 A convincing browser or OS update prompt is shown
4 CornFlake installs, posing as a cloud sync Windows service
5 Device-code flow abused to reach the accounts behind the device

ASSESSMENT, LESSONS, AND RECOMMENDATIONS

- The user did nothing wrong - no email, no link. Awareness alone cannot reach this.
- Attribution is layered: APT29 to the SVR is a government position; this campaign to Storm-2945 is Microsoft's.
- How the gateways were first compromised is unexplained, so no venue can be confident it is unaffected.
- It is almost certain that Russian state actors keep targeting travelling officials through the networks they depend on abroad.