PRIMUS PARTNERS®

Quote by Devroop Dhar, Co-Founder & India CEO, Primus Partners

Published in CSO Online
April 08, 2026 | 02:30 PM IST

Forest Blizzard leverages router compromises to launch AiTM attacks, target Outlook sessions

Authored by Nidhi Singhal

Read on: Forest Blizzard leverages router compromises to launch AiTM attacks, target Outlook sessions | CSO Intel, AI, labour

Article Content:

By altering DNS settings on vulnerable devices, Forest Blizzard redirects users to malicious infrastructure to capture credentials and session data, says Microsoft Threat Intelligence.

Russian threat actor Forest Blizzard has been exploiting unsecured home and small-office internet equipment, such as routers, to redirect traffic through attacker-controlled DNS servers.

The group has leveraged this DNS hijacking activity to support post-compromise adversary-in-the-middle (AiTM) attacks on Transport Layer Security (TLS) connections, targeting Microsoft Outlook on the web domains, according to a Microsoft Threat Intelligence report. By compromising upstream edge devices, the attackers are able to exploit less monitored networks and use them as a pathway to access enterprise environments.

More than 200 organizations and over 5,000 consumer devices have already been impacted by Forest Blizzard's malicious DNS infrastructure, which Microsoft says is primarily used to

collect intelligence in support of the Russian government's foreign policy objectives. The activity enables interception of cloud-hosted content, with government, IT, telecommunications, and energy sectors among the primary targets.

While the number of organizations specifically targeted for TLS AiTM is only a subset of the networks with vulnerable SOHO devices, the threat actor's broad access could enable larger-scale AiTM attacks, which might include active traffic interception, Microsoft said in the blog post.

Hijacked routers, stolen sessions

Forest Blizzard, also called APT28 by the UK's National Cyber Security Center, broke into home and small-office routers and changed their network settings so that internet traffic was sent through their own DNS servers. For this, the threat actor almost certainly used the dnsmasq utility to perform DNS resolution and provide responses while listening to port 53 for DNS queries, Microsoft Threat Intelligence noted.

Most of the time, attackers quietly monitored traffic without disrupting connections. But for specific targets, they spoofed DNS responses and actively redirected users to the fake infrastructure they controlled. These included a subset of domains associated with Microsoft Outlook on the web. Separate AiTM activity targeting non-Microsoft hosted servers in at least three government organizations in Africa was also identified.

"The actor-controlled malicious infrastructure would then present an invalid TLS certificate to the victim, spoofing the legitimate Microsoft service. If the compromised user ignored warnings about the invalid TLS certificate, the threat actor could then actively intercept the underlying plaintext traffic — potentially including emails and other customer content — within the TLS connection," claimed the blog post.

Invisible path to enterprise systems

This attack poses a serious risk to enterprises because, instead of beginning at the corporate perimeter, it starts from employee environments that are often less secure. Threat actors target vulnerable home or small office routers, which often have weak default passwords or unpatched software.

The shift to remote work has dramatically expanded the corporate attack surface, allowing attackers to create a pathway into enterprise accounts without directly breaching corporate systems.

"The real-world impact is profound. Attackers can intercept credentials, reroute traffic to malicious sites, or inject malware, all without ever breaching the corporate firewall. This can lead to data breaches, financial theft, or even ransomware incidents originating from an employee's living room," said Apeksha Kaushik, senior principal analyst at Gartner. "Moreover, the lack of visibility and control over home networks means these attacks can persist undetected, undermining even the most robust corporate security programs. In essence, every unsecured home network becomes a potential backdoor into the enterprise, amplifying risk and complicating incident response."

Defending beyond corporate networks

For CISOs, this broadens the focus area beyond merely securing corporate networks and even addressing risks in employee home environments and unmanaged devices.

"First, stop using passwords. Robust two-step verification systems that do not allow for phishing attacks, especially hardware tokens, could prevent most of these attacks despite credentials being obtained," said Devroop Dhar, CEO and co-founder at Primus Partners.

Dhar added that CISOs should look at controlling the behaviour of identities. For instance, if there is an unusual location or device involved in the login procedure, additional warnings or checks need to be generated.

"Enforce secure DNS solutions by utilizing corporate VPNs with split tunneling disabled or enforcing DNS over HTTPS to ensure all DNS queries bypass the local home router and go directly to trusted corporate servers," suggested Amit Jaju, global partner at Ankura Consulting. "Also, implement strict conditional access policies that require devices to be enrolled in mobile device management and marked as compliant before granting access to corporate cloud resources."

Experts also warn that even after taking all precautions and defence measures, educating employees should be the utmost priority, as they must be trained to recognize suspicious behaviour during login procedures.