CSAI Foundation

Cloud Security Alliance AI Safety Initiative

FrostArmada: Forest Blizzard SOHO Router OAuth Token Harvest

GRU DNS Hijacking via Compromised Edge Devices Enables Nation-State AiTM Credential Theft

Unofficial AI-assisted Research

2026-04-11

Key Takeaways

On April 7, 2026, the U.S. Department of Justice, FBI, and UK National Cyber Security Centre (NCSC) published coordinated advisories attributing a large-scale credential-harvesting campaign—codenamed FrostArmada by Lumen's Black Lotus Labs—to APT28 (also known as Forest Blizzard, Fancy Bear, and Sofacy Group), a threat actor associated with GRU Military Unit 26165 of Russia's Main Intelligence Directorate [1][2][3]. The campaign, active since at least May 2025, exploited known vulnerabilities in TP-Link and MikroTik SOHO routers to alter DHCP and DNS configurations, redirecting all connected devices to actor-controlled DNS resolvers without victim awareness [2][5]. Through real-time adversary-in-the-middle (AiTM) proxy infrastructure, GRU actors completed MFA challenges on behalf of victims and captured the resulting OAuth access tokens and session cookies for replay against legitimate Microsoft 365 services—intercepting post-authentication credential artifacts that services accept as proof of completed MFA verification [4]. At its peak in December 2025, more than 18,000 unique IP addresses from at least 120 countries communicated with Forest Blizzard's malicious DNS infrastructure; Microsoft Threat Intelligence identified over 200 organizations and 5,000 consumer devices impacted by the campaign [1][4][5]. Primary targets included ministries of foreign affairs, law enforcement agencies, and third-party cloud service providers across North Africa, Central America, Southeast Asia, and Europe [1][2]. The FBI conducted a court-authorized technical operation (Operation Masquerade) to neutralize the U.S. portion of the compromised router network [3].

Two aspects of the campaign deserve particular attention. First, exploitation surged in August 2025 in the days following public disclosure of an NCSC advisory—a pattern consistent with adversary groups adapting in near real-time to published threat intelligence [5]. Second, the campaign draws a consequential distinction among MFA mechanisms: TOTP, SMS-based OTP, and push notification factors are equally vulnerable to AiTM proxy interception, while phishing-resistant FIDO2/WebAuthn mechanisms provide structural resistance by binding authentication assertions to the target origin, so that a victim connecting to a malicious proxy cannot produce an assertion valid for the legitimate service [14]. Organizations relying on MFA as their sole credential defense should treat this campaign as a clear signal that authentication token security demands the same rigor as password security. The sections that follow examine the FrostArmada attack chain in detail, assess the structural conditions that enabled it, and provide prioritized recommendations and CSA framework alignment for organizations seeking to reduce their exposure.

Background

APT28 has operated on behalf of Russian military intelligence for more than a decade, conducting cyber espionage against government institutions, defense contractors, political organizations, and critical infrastructure globally. The group's technical sophistication is well-documented, spanning phishing campaigns, credential-stealing implants, exploitation of zero-day vulnerabilities, and large-scale infrastructure hijacking operations [11]. Forest Blizzard is a sub-designation applied by Microsoft Threat Intelligence to track GRU Unit 26165 activity with particular focus on authentication credential theft and cloud-service intrusion.

The FrostArmada campaign represents a tactical evolution in how Forest Blizzard achieves persistent, passive intelligence collection at scale. Rather than deploying malware on target endpoints—which would expose indicators of compromise and risk detection by endpoint security tools—the actors appear to have opted to operate upstream, at the network infrastructure layer, in an environment where visibility and patch cadence are typically weakest [4]. This approach is consistent with a deliberate effort to minimize the operational footprint that forensic and network security tools are most likely to surface. SOHO routers are frequently purchased once and left unmanaged for years; they run outdated firmware, expose administrative interfaces to the public internet, and retain factory-default credentials. This makes them attractive footholds for nation-state actors who require persistent, low-noise collection infrastructure.

The campaign's operational timeline, as reconstructed from law enforcement and vendor intelligence, began with limited exploitation activity in May 2025. Widespread router compromise accelerated in early August 2025 and reached peak scale in December 2025. At that point, Lumen's Black Lotus Labs detected more than 18,000 unique IP addresses from over 120 countries actively communicating with Forest Blizzard's DNS infrastructure [5]. The coordinated law enforcement and advisory response in April 2026—encompassing advisories from the DOJ, FBI IC3, and NCSC, among others [3][6]—indicates both the maturation of the threat and the severity of the intelligence collection that prompted it.

The router models targeted span a wide range of TP-Link consumer and SMB devices—including the WR841N, WR840N, WR842N, WR845N, WR941ND, WR1043ND, Archer C5, Archer C7, WDR3500, WDR3600, and WDR4300 lines, as well as MR3420 and MR6400 LTE routers—alongside MikroTik devices running RouterOS [1][2]. Several of these models are at or near end-of-support, meaning vendor-issued security patches are no longer available, and devices in this product family are known to persist in deployed networks well past their vendor support lifecycle.

Security Analysis

Attack Chain: From Router to OAuth Token

The FrostArmada attack chain is notable for its simplicity and leverage. Forest Blizzard first obtained router credentials by exploiting known vulnerabilities, most prominently CVE-2023-50224, a flaw in the TP-Link WR841N that allows an unauthenticated attacker to extract password credentials via specially crafted HTTP GET requests [1][2]. After gaining administrative access, the actors issued a second crafted HTTP GET request to modify the router's DHCP configuration, replacing the legitimate primary DNS server address with an IP address under GRU control while demoting the original DNS server to secondary fallback [2]. This modification is inherited automatically by every device connected to the compromised router—laptops, mobile phones, servers—without any action required on the part of those devices' owners.

Downstream devices then directed all DNS resolution queries to GRU-controlled virtual private servers running the dnsmasq utility. Dnsmasq is a widely used, lightweight DNS forwarding and caching daemon that is entirely legitimate in normal router operation; its presence on the actor's collection servers provided no inherent indication of compromise to network monitoring tools scanning for known malware signatures [4][5]. Forest Blizzard is assessed with high confidence to be using dnsmasq, listening on port 53, to perform DNS resolution and return responses to downstream victims [4].

The actor then applied automated filtering to the DNS request stream. The vast majority of DNS queries were forwarded legitimately—a selective approach that would limit anomalous traffic volumes and reduce the likelihood of detection by network operators. Only queries for domains associated with specific authentication services—particularly subdomains of Microsoft Outlook on the Web, Office 365, and related Microsoft cloud identity infrastructure—triggered a different response: the GRU's DNS resolver returned a fraudulent IP address pointing to actor-controlled proxy infrastructure rather than to Microsoft's actual servers [2][3][4]. Victims attempting to authenticate to these services were directed, entirely transparently from their perspective, to a real-time AiTM proxy that relayed their credentials and MFA challenge responses to the legitimate Microsoft service, completed the authentication on their behalf, and captured the resulting OAuth access token and session cookie [4].

The implications of this technique merit careful attention. OAuth tokens and session cookies represent post-authentication state—they are the artifacts that services accept as proof that a legitimate authentication, including MFA verification, has already occurred. Once an actor possesses a valid token, they can access the associated account from any IP address, at any time, without triggering further authentication challenges, for the duration of the token's validity period. Forest Blizzard used this technique to circumvent MFA's core protection: rather than stopping at the MFA challenge, the AiTM

proxy completed authentication on the victim's behalf and captured the resulting token. In this attack scenario, MFA verification occurred but delivered its credential artifact directly to the attacker, leaving post-authentication access control as the only remaining defense [4][5].

Selective Targeting and Collection Discipline

A notable operational characteristic of the FrostArmada campaign was its discipline in applying selective targeting. Despite compromising routers across 120 countries, the actors did not attempt to intercept all traffic flowing through their infrastructure—an approach that would have been impractical to manage and far more likely to generate anomalous traffic volumes detectable by network operators [2]. Instead, keyword-based filtering on DNS query content allowed the actors to identify which DNS requests were associated with intelligence-priority domains and to activate AiTM interception only for those queries. This selective approach enabled the campaign to operate for approximately eleven months before large-scale disruption in April 2026, with peak collection infrastructure active from approximately August through December 2025.

Microsoft confirmed that its own infrastructure and services were not directly compromised; the campaign's impact was on the users and organizations connecting to Microsoft services through poisoned DNS infrastructure [4]. This pattern is consistent with a signals intelligence collection objective: passive, large-scale credential harvesting in support of follow-on espionage against high-value diplomatic, law enforcement, and governmental targets, rather than any disruptive or destructive end.

Why SOHO Devices Represent Structural Risk

The exploitation of SOHO infrastructure for intelligence collection is not unique to this campaign—VPNFilter and the Volt Typhoon router botnet established this methodology in prior operations, demonstrating that SOHO devices have become a preferred tier in advanced adversary infrastructure. FrostArmada reinforces that assessment by achieving persistent, low-detection-risk access at a scale that would be considerably harder to sustain through endpoint-focused tradecraft. SOHO routers occupy a position of implicit trust in most network architectures: they are upstream of all user traffic, they manage DNS resolution for every connected device, and their administrative interfaces are rarely monitored. Yet they are also among the most poorly maintained assets in any organization's inventory. Patch cycles are irregular or nonexistent, default credentials are frequently retained, and remote management interfaces are commonly exposed to the internet despite published CISA and vendor guidance recommending that administration be restricted to the local network [12].

The structural risk extends beyond this specific campaign. Any nation-state or sophisticated criminal actor with similar resource levels can apply the same technique to compromised SOHO infrastructure to conduct large-scale credential collection against any cloud-hosted service that relies on password or token-based authentication. The FrostArmada campaign should therefore be understood not as an isolated incident but as a demonstration of a repeatable, scalable, difficult-to-detect collection methodology that will persist as a threat vector as long as SOHO infrastructure remains under-managed.

Recommendations

Immediate Actions

Organizations and individuals operating SOHO routers should take the following steps without delay. First, verify that all routers—particularly TP-Link and MikroTik devices—are running the latest available firmware. Where the manufacturer has discontinued support for the device model, replace the hardware with a currently supported alternative [7][12]. Second, change all router administrative credentials from factory defaults; default credentials for affected TP-Link models are widely known and exploited trivially. Third, disable remote management interfaces from the public internet; router administration should be accessible only from the local network. Fourth, review current DHCP and DNS server settings on all managed routers and compare them against expected values; any DNS server entry pointing to an unfamiliar IP address should be treated as a potential indicator of compromise [1][2].

Short-Term Mitigations

Security teams should augment router hardening with network-layer defenses designed to limit the effectiveness of DNS hijacking. Deploying encrypted DNS protocols—specifically DNS over HTTPS (DoH) or DNS over TLS (DoT)—on client devices significantly reduces the risk of DNS query interception in this attack model, provided the client is configured to use a hardcoded trusted resolver rather than the network-assigned one [13]. When clients resolve DNS through a direct, encrypted connection to a known provider, a compromised upstream DHCP/DNS configuration cannot silently redirect those queries. Organizations should also implement DNSSEC validation on endpoints where feasible, which provides cryptographic verification of DNS record authenticity.

From an identity and access management perspective, organizations should audit OAuth token lifetimes and session persistence policies. Long-lived tokens and persistent sessions significantly extend the window of exploitation once a token is captured; reducing token expiry and requiring re-authentication

for sensitive operations limits the value of harvested credentials. Conditional access policies that enforce device compliance and geolocation anomaly detection can flag replay attacks in which a harvested token is used from an unexpected IP address or geographic region [4].

Network monitoring capabilities should be extended to cover DNS traffic patterns. Anomalous DNS resolution behavior—particularly queries resolving authentication-related domains to unexpected IP addresses—can indicate a compromised upstream resolver and warrants immediate investigation. Organizations with the capability to monitor DHCP lease assignments should alert on unexpected changes to DNS server configuration in router DHCP responses.

Strategic Considerations

At a strategic level, FrostArmada underscores the inadequacy of treating MFA as a complete credential security solution. As the campaign demonstrates, AiTM proxy techniques can neutralize time-based one-time passwords (TOTP), SMS-based OTP, and application push notification factors equally. Phishing-resistant MFA mechanisms—specifically FIDO2/WebAuthn hardware security keys and passkeys bound to the authenticating device—are substantially harder to compromise through AiTM proxying because they incorporate the origin (the target domain) as part of the authentication assertion. Victims authenticating to a malicious proxy site cannot generate a valid FIDO2 assertion for the legitimate target domain, causing authentication to fail before credentials are disclosed [8][14]. Security programs that have not yet migrated high-value accounts to phishing-resistant MFA should prioritize this transition, beginning with administrator accounts and users with access to sensitive communications.

Network segmentation and Zero Trust architecture principles provide additional defense in depth. By treating every network request as potentially traversing untrusted infrastructure and enforcing authentication at the application layer rather than at the network perimeter, organizations reduce their dependence on the integrity of SOHO and edge devices that cannot be reliably managed. In practice, this means deploying Zero Trust Network Access (ZTNA) solutions that authenticate and authorize each connection independently, rather than assuming that a device on the local network or connected through a corporate VPN is inherently trustworthy.

CSA Resource Alignment

The FrostArmada campaign sits at the intersection of several CSA research domains, and existing CSA frameworks provide directly applicable guidance for organizations responding to this threat.

Zero Trust Architecture. CSA's Zero Trust Working Group has published extensive guidance on implementing Zero Trust principles across enterprise and SMB environments. The Zero Trust Guidance for Small and Medium-Sized Businesses is particularly relevant, as it addresses the specific constraints of organizations that may lack dedicated security operations capacity. The core Zero Trust principle—never trust, always verify—directly addresses the threat posed by compromised upstream DNS infrastructure: when application-layer authentication does not depend on network-layer trust, DNS hijacking at the router level becomes substantially less effective as an attack vector. An attacker who redirects DNS cannot easily obtain valid credentials if the authentication protocol validates endpoint identity through mechanisms—such as FIDO2 or certificate-based mutual authentication—that the attacker cannot forge [9]. CSA's five-step Zero Trust implementation process (define the protect surface, map operational flows, build a ZTA, create policies, monitor and maintain) provides a practical framework for organizations seeking to reduce their exposure to this class of attack.

Cloud Controls Matrix (CCM) v4.0. Several control domains within CCM v4.0 speak directly to the vulnerabilities exploited in FrostArmada. The Identity and Access Management (IAM) domain addresses token lifecycle management, session security, and multi-factor authentication requirements that, if implemented to the control specifications, would have materially limited the value of harvested OAuth tokens. The Infrastructure and Virtualization Security (IVS) domain covers network security baselines, including DNS security controls, that address the router configuration weaknesses central to this campaign. Organizations conducting STAR assessments should treat IAM and IVS controls related to token security and DNS integrity as priority items in the current threat environment.

Software-Defined Perimeter (SDP) Architecture. CSA's SDP Architecture Guide describes an authenticate-before-connect model that, by design, does not allow any network connection to occur before device and user identity have been verified through a strong cryptographic handshake [10]. In an SDP model, the network infrastructure layer—including potentially compromised SOHO routers—does not have visibility into which services a user is attempting to reach until authentication has already succeeded. The cryptographic Single Packet Authorization (SPA) handshake that precedes service-directed DNS queries substantially reduces the attack surface available to DNS hijacking. Organizations deploying SDP should verify that authentication endpoint discovery itself uses encrypted or hardcoded DNS, so that the initial connection to the SPA gateway is not itself subject to DNS poisoning. CSA's Stealth Mode SDP guidance extends this approach by eliminating the discoverability of protected infrastructure entirely.

AI Organizational Responsibilities. While FrostArmada is not an AI-enabled attack, AI-augmented analytics are increasingly applied to detecting the behavioral anomalies—unusual OAuth token usage patterns, geolocation discrepancies, DNS resolution deviations—that characterize post-exploitation

activity following a successful token harvest. Organizations integrating AI-based security operations tooling should ensure that OAuth token telemetry is included in behavioral baselines and that anomaly detection thresholds for token replay are appropriately calibrated.

References

[1] UK National Cyber Security Centre (NCSC). "APT28 Exploit Routers to Enable DNS Hijacking Operations." NCSC.gov.uk, April 8, 2026.

[2] The Hacker News. "Russian State-Linked APT28 Exploits SOHO Routers in Global DNS Hijacking Campaign." The Hacker News, April 2026.

[3] U.S. Department of Justice. "Justice Department Conducts Court-Authorized Disruption of DNS Hijacking Network Controlled by a Russian Military Intelligence Unit." DOJ Office of Public Affairs, April 7, 2026.

[4] Microsoft Threat Intelligence. "SOHO Router Compromise Leads to DNS Hijacking and Adversary-in-the-Middle Attacks." Microsoft Security Blog, April 7, 2026.

[5] Lumen Technologies / Black Lotus Labs. "FrostArmada: Forest Blizzard DNS Hijacking." Lumen Blog, April 2026.

[6] FBI Internet Crime Complaint Center (IC3). "Russian GRU Exploiting Vulnerable Routers to Steal Sensitive Information." IC3 PSA, April 7, 2026.

[7] BleepingComputer. "Authorities Disrupt Router DNS Hijacks Used to Steal Microsoft 365 Logins." BleepingComputer, April 2026.

[8] SecurityWeek. "US Disrupts Russian Espionage Operation Involving Hacked Routers and DNS Hijacking." SecurityWeek, April 2026.

[9] Cloud Security Alliance. "Zero Trust Working Group." Cloud Security Alliance, accessed April 2026.

[10] Cloud Security Alliance. "Software-Defined Perimeter Architecture Guide." Cloud Security Alliance, accessed April 2026.

[11] MITRE ATT&CK. "APT28 (Group G0007)." MITRE ATT&CK, accessed April 2026.

[12] Cybersecurity and Infrastructure Security Agency (CISA) and FBI. "Security Guidance for SOHO Routers." CISA, January 2024.

[13] Internet Engineering Task Force. "DNS Queries over HTTPS (DoH), RFC 8484." IETF, October 2018.

[14] Cybersecurity and Infrastructure Security Agency (CISA). "Implementing Phishing-Resistant MFA." CISA, October 2022.