INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-04-09 06:07 UTC

APT28 (Forest Blizzard) Conducts Credential Theft via SOHO Router DNS Hijacking

THREAT CAMPAIGN | **HIGH** | CVSS 7.5

SCC Item ID	SCC-CAM-2026-0160
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	7.5
Affected Products	SOHO routers, specific vendors and models not identified in available source material; broad deployment across organizations and remote worker environments
Published	2026-04-08T21:00:00
Discovery Source	Rss

Executive Summary

APT28 (Forest Blizzard), a Russian state-sponsored threat group, is actively compromising SOHO routers to redirect authentication traffic through attacker-controlled infrastructure, intercepting credentials without placing any malware on target networks. Any organization relying on SOHO routers, including remote worker environments, is exposed if those devices run default or weak management credentials or unpatched firmware. The business risk is credential theft at scale: valid user credentials harvested through this technique enable follow-on intrusion into corporate systems, cloud services, and VPNs without triggering endpoint-based alerts.

Technical Analysis

APT28/Forest Blizzard is modifying DNS resolver settings on compromised SOHO routers to redirect authentication traffic to adversary-controlled infrastructure, executing adversary-in-the-middle (AiTM) credential interception. No endpoint payload is deployed; the attack operates entirely at the network management plane. Initial access to the router exploits weak or default management credentials and unpatched firmware; no specific CVE has been identified in available source material as the entry vector. Once DNS settings are modified, downstream clients transparently resolve authentication endpoints to attacker-controlled IPs, enabling credential capture across all devices on the affected network segment. Relevant CWEs: CWE-300 (Channel Accessible by Non-Endpoint), CWE-16 (Configuration), CWE-287 (Improper Authentication). MITRE ATT&CK coverage: T1557 (Adversary-in-the-Middle), T1584.002 (Compromise Infrastructure: DNS Server), T1584.008 (Compromise Infrastructure: Network Devices), T1556 (Modify Authentication Process), T1562.001 (Impair Defenses: Disable or Modify Tools), T1078 (Valid Accounts), T1133 (External Remote Services), T1040

(Network Sniffing), T1071.001 (Application Layer Protocol: Web Protocols). Specific affected router vendors and firmware versions are not identified in available source material. Attribution sourced from Microsoft Security Blog, April 7, 2026.

Action Checklist

1. Step 1, Immediate Containment: Audit DNS resolver settings on all SOHO routers in corporate and remote worker environments. Compare current DNS server entries against known-good baseline values (typically ISP-assigned or organization-approved resolvers). Any unknown or external DNS IP should be treated as a compromise indicator and the device isolated from the network pending investigation. Prioritize routers with internet-exposed management interfaces.
2. Step 2, Detection: Query DNS logs and firewall flow data for outbound DNS traffic destined to resolvers outside approved ranges. Look for authentication traffic (HTTP 401/302 flows, NTLM or Kerberos exchanges) routed to unexpected upstream IPs. Review router access logs for management-plane logins, configuration changes, and firmware modifications. SIEM query focus: DNS resolver change events, anomalous authentication redirect patterns, and unexpected management-plane access. No published IOC hashes or IPs are available in current source material; flag any unrecognized DNS resolver IP as high-priority for investigation.
3. Step 3, Eradication: Change all router management credentials from default or weak values to unique, strong passwords. Disable remote management interfaces where not operationally required. Apply all available firmware updates from the device vendor. Restore DNS resolver settings to known-good values. Where firmware is end-of-life with no available patch, prioritize device replacement. Consult your specific router vendor's advisory for firmware version guidance; vendor-specific patch IDs are not identified in current source material.
4. Step 4, Recovery: After remediation, verify DNS resolver settings have not reverted. Monitor authentication logs for credential reuse attempts using accounts that may have been exposed during the compromise window. Force password resets for any accounts that authenticated through affected network segments during the suspected compromise period. Validate MFA enforcement on all externally accessible services and VPNs to limit the impact of harvested credentials.
5. Step 5, Post-Incident Analysis: This campaign exposes three control gaps: (1) absence of network-layer DNS monitoring, (2) no baseline integrity checks for router configuration, and (3) lack of MFA on services reachable via harvested credentials. Remediation investments should include DNS query logging with anomaly detection, automated router configuration compliance checks, and MFA enforcement across all authentication paths. Map control improvements to NIST CSF PR.AC, DE.CM, and RS.MI categories.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE

Escalation Criteria	Escalate to senior leadership, legal counsel, and (if applicable) CISA immediately if: any authentication log evidence confirms that credentials harvested via the APT28 DNS hijack were successfully reused to access corporate systems, cloud tenants, or VPNs; if any affected accounts have access to PII, PHI, or financial data triggering state breach notification laws or HIPAA/PCI DSS reporting obligations; or if the organization's incident response team lacks the capacity to audit all SOHO routers within 24 hours given the active, ongoing nature of this APT28 campaign.
Recovery Notes	After router remediation and credential resets, maintain elevated monitoring of authentication logs (Windows Security Event IDs 4624, 4625, 4648, 4768, 4769, 4776) for all accounts that authenticated through affected network segments during the compromise window for a minimum of 90 days, as APT28 is known to stockpile credentials for delayed use aligned with operational objectives. Verify weekly for the first month that DNS resolver settings on all remediated routers have not reverted, using the automated hash-comparison or SSH-pull script established in the post-incident controls; any reversion indicates the attacker has regained management-plane access and the device must be re-isolated and re-imaged. Confirm that MFA enforcement on all externally accessible services — particularly VPN gateways and OWA/M365 — is validated by a test authentication attempt, not merely by policy review, before declaring the incident closed.
Forensic Artifacts	Router running configuration export (pre-reset): Contains the attacker-modified DNS resolver IP fields — the primary evidence of APT28's DNS hijack; preserve as a timestamped file with SHA-256 hash before any remediation action is taken. | Router syslog / system event log: Contains management-plane login events (successful logins from non-RFC1918 or unexpected external IPs) and configuration-change events timestamped immediately after those logins — reconstructs APT28's initial access and DNS modification sequence. | WAN-side pcap (tcpdump on router WAN interface or upstream firewall span port, port 53): Captures the attacker-controlled resolver IP receiving all outbound DNS queries from the network — the primary network-layer IOC given no published APT28 resolver IPs are available in current source material. | Windows Security Event Log (Event IDs 4648, 4776, 4768, 4769) from endpoints that authenticated to corporate services during the compromise window: Reveals whether NTLM or Kerberos authentication traffic was intercepted by APT28 infrastructure during the DNS hijack period, establishing the scope of credential exposure. | Firewall/NAT session table and port-forwarding rule export at time of detection: APT28 may have added persistent port-forwarding rules to the hijacked router (e.g., forwarding management ports to an internal pivot host) beyond the DNS change; this artifact captures any secondary persistence mechanisms installed during their access window.

Per-Action IR Details

Step 1: Containment — Immediately audit DNS resolver settings on all SOHO routers in corporate and remote worker environments. Compare current DNS server entries against known-good baseline values (typically ISP-assigned or organization-approved resolvers). Any unknown or external DNS IP should be treated as a compromise indicator and the device isolated from the network pending investigation. Prioritize routers with internet-exposed management interfaces.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy

Controls: NIST IR-4 (Incident Handling), NIST SI-4 (System Monitoring), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 4.2 (Establish and Maintain a Secure Configuration Process for Network Infrastructure)

Compensating: For each SOHO router, SSH or access the web management interface and dump the current DNS resolver entries: on Linux-based router firmware (e.g., OpenWRT) run 'cat /etc/resolv.conf' and 'uci show network |

grep dns'; on consumer firmware access System > WAN settings and screenshot DNS fields. Compare output against a pre-built text file of approved resolver IPs (ISP-assigned primaries plus any org-approved forwarders like 9.9.9.9 if intentionally deployed). Flag any IP not in that list. For remote workers, deploy a one-time PowerShell check from a central script: 'Get-DnsClientServerAddress | Where-Object {$_.ServerAddresses -notmatch ""}' to surface endpoints whose upstream DNS has been redirected. Isolate flagged routers by placing them on a quarantine VLAN or physically disconnecting WAN uplinks before proceeding.

Evidence: Before isolating any router, preserve the current running configuration in full: export the router's startup and running config via CLI ('show running-config' on Cisco-based, 'nvram show' on DD-WRT, full config backup via vendor web UI) and capture the WAN DNS resolver fields with a timestamped screenshot. Export the router's system log (typically syslog or /var/log/messages on Linux-based firmware) covering at minimum the past 30 days — APT28's DNS hijack involves management-plane access to change resolver settings, so look for configuration-change log entries showing DNS field modifications paired with admin login events from unexpected source IPs. Capture the ARP table ('arp -a' or 'ip neigh show') and active connections table at time of isolation to document any persistent C2 sessions the attacker may have maintained to the router's management interface.

Step 2: Detection — Query DNS logs and firewall flow data for outbound DNS traffic destined to resolvers outside approved ranges. Look for authentication traffic (HTTP 401/302 flows, NTLM or Kerberos exchanges) routed to unexpected upstream IPs. Review router access logs for management-plane logins, configuration changes, and firmware modifications. SIEM query focus: DNS resolver change events, anomalous authentication redirect patterns, and unexpected management-plane access. No published IOC hashes or IPs are available in current source material; flag any unrecognized DNS resolver IP as high-priority for investigation.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis

Controls: NIST AU-2 (Event Logging), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST SI-4 (System Monitoring), CIS 8.2 (Collect Audit Logs), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Without a SIEM, run detection in three discrete steps. (1) DNS resolver audit: on each router pull the current DNS config as described in Step 1 and diff against your approved baseline file using 'diff approved_resolvers.txt current_resolvers.txt'. (2) Outbound DNS flow analysis: capture 15-30 minutes of WAN-side traffic with 'tcpdump -i eth0 port 53 -w dns_capture.pcap' and open in Wireshark; filter on 'dns' and inspect the destination IPs of all queries — any destination not matching your approved resolver IPs is a finding. (3) Authentication redirect detection: filter the pcap further with 'http.response.code == 401 || http.response.code == 302' and inspect the IP of the server issuing those responses; in APT28's DNS hijack model, HTTP 401/302s for corporate services will originate from the attacker-controlled resolver's associated infrastructure rather than the legitimate service IP. For router management-plane review, pull syslog entries and grep for keywords: 'grep -iE "login|config|dns|passwd|admin" /var/log/messages' — look for successful logins from non-RFC1918 source IPs or outside business hours.

Evidence: Preserve the following before any remediation action: (1) Full pcap of outbound DNS queries from the WAN interface for the detection window — this captures which resolver IP APT28 configured and is receiving queries, which is your primary network-layer IOC given no published IPs exist in current source material. (2) Router syslog or system event log showing timestamps of any DNS configuration change events, admin login events (successful and failed), and firmware-related entries — APT28's initial access to the router's management plane will appear here as a login from an unexpected external IP followed immediately by a configuration write event. (3) Windows Security Event Log (Event ID 4648 — Logon using explicit credentials, and Event ID 4776 — NTLM authentication) from any endpoint that authenticated to corporate services during the suspected compromise window; if DNS was hijacked, NTLM challenges may have been relayed to APT28 infrastructure, making these logs evidence of credential exposure scope. (4) Firewall/NAT table at time of detection showing any persistent external sessions to the router's management port (typically TCP 80, 443, or 8080/8443 for web UI; TCP 22 for SSH).

Step 3: Eradication — Change all router management credentials from default or weak values to unique, strong passwords. Disable remote management interfaces where not operationally required. Apply all available firmware updates from the device vendor. Restore DNS resolver settings to known-good values.

Where firmware is end-of-life with no available patch, prioritize device replacement. Consult your specific router vendor's advisory for firmware version guidance — vendor-specific patch IDs are not identified in current source material.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST SI-2 (Flaw Remediation), NIST CM-6 (Configuration Settings), NIST IA-5 (Authenticator Management), CIS 4.7 (Manage Default Accounts on Enterprise Assets and Software), CIS 5.2 (Use Unique Passwords), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management)

Compensating: Eradication for a 2-person team with no enterprise tooling proceeds device-by-device: (1) Factory reset the router to clear any APT28-persisted configuration (hold reset button per vendor instructions) — do not simply restore a saved config backup that predates your baseline comparison, as the compromise window may predate your most recent backup. (2) After reset, before reconnecting WAN, change the default admin credential to a unique strong password (minimum 16 characters, alphanumeric + special), disable the remote management interface (typically 'Remote Management' toggle in WAN or Administration settings), and manually re-enter only the approved DNS resolver IPs. (3) Download the latest firmware from the vendor's official support portal (not from any URL served during the compromise window, as DNS hijacking could have poisoned firmware download URLs) and apply it before the device goes back online. (4) Document each router's new credentials in a password manager (Bitwarden is free and suitable) with a per-device entry. (5) For EOL devices with no firmware update available, treat replacement as a P1 procurement action and place an ACL-enforced compensating control at the upstream firewall or managed switch to block inbound TCP 80/443/22/8080/8443 to the router's management IP until replacement hardware arrives.

Evidence: Before factory reset, capture: (1) Full running config export showing the attacker-configured DNS resolver IPs — this is your primary eradication confirmation artifact; after reset and reconfiguration, re-export the config and diff to confirm DNS fields now match approved values and no other unexpected entries (static routes, port forwards, or DDNS entries) were introduced by APT28 during their access window. (2) Firmware version string from the pre-reset management UI or CLI ('show version' or equivalent) — document the vulnerable firmware version for your post-incident report and to support any vendor or CISA reporting obligations. (3) Any port forwarding or DMZ rules visible in the pre-reset config — APT28 may have added persistent access rules (e.g., forwarding TCP 22 or 8080 to an internal pivot host) beyond the DNS change itself.

Step 4: Recovery — After remediation, verify DNS resolver settings have not reverted. Monitor authentication logs for credential reuse attempts using accounts that may have been exposed during the compromise window. Force password resets for any accounts that authenticated through affected network segments during the suspected compromise period. Validate MFA enforcement on all externally accessible services and VPNs to limit the impact of harvested credentials.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST IR-4 (Incident Handling), NIST IA-5 (Authenticator Management), NIST AU-6 (Audit Record Review, Analysis, and Reporting), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.4 (Require MFA for Remote Network Access), CIS 6.5 (Require MFA for Administrative Access), CIS 5.2 (Use Unique Passwords)

Compensating: Recovery verification for a 2-person team: (1) DNS reversion check — 48 hours after remediation, re-query each router's DNS settings via the management interface and diff against the approved baseline file; schedule this as a weekly cron job using a simple bash script that SSHs to each router (using key-based auth established during eradication), pulls the DNS config, and emails a diff report. (2) Credential reuse monitoring — pull Active Directory Security Event Logs for Event ID 4625 (Failed Logon) and Event ID 4768 (Kerberos TGT Request) filtered to usernames known to have authenticated through the affected network segments; look for authentication attempts from unexpected source IPs or geolocations, which would indicate APT28 is attempting to leverage harvested credentials. Use 'Get-EventLog -LogName Security -InstanceId 4625 -After ' in PowerShell to scope the review. (3) MFA gap identification — for each externally accessible service (VPN, Outlook Web Access, RDP Gateway, cloud apps), attempt a test authentication with a non-MFA-enrolled test account to confirm MFA is enforced; document any service that does not challenge for a second factor as a P1 remediation gap.

Evidence: During the recovery phase, preserve: (1) Authentication logs (Windows Security Event Log Event IDs 4624, 4625, 4648, 4768, 4769, 4776) from the first 30 days post-remediation, filtered to accounts identified as exposed during the compromise window — unusual logon times, source IPs, or service names in these logs are evidence of active credential reuse by APT28. (2) VPN and remote access gateway authentication logs for the same exposed account list and time window — APT28 credential reuse against VPNs is a documented follow-on behavior consistent with their credential-harvesting objectives. (3) A post-remediation DNS resolver configuration export from each router taken at 24-hour and 7-day intervals, retained as evidence that the attacker has not regained access and re-hijacked DNS settings.

Step 5: Post-Incident — This campaign exposes three control gaps: (1) absence of network-layer DNS monitoring, (2) no baseline integrity checks for router configuration, and (3) lack of MFA on services reachable via harvested credentials. Remediation investments should include DNS query logging with anomaly detection, automated router configuration compliance checks, and MFA enforcement across all authentication paths. Map control improvements to NIST CSF PR.AC, DE.CM, and RS.MI categories.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity

Controls: NIST IR-4 (Incident Handling), NIST IR-8 (Incident Response Plan), NIST AU-2 (Event Logging), NIST SI-7 (Software, Firmware, and Information Integrity), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process), CIS 8.2 (Collect Audit Logs)

Compensating: Post-incident control improvements achievable by a 2-person team at no cost: (1) DNS monitoring — deploy Pi-hole or a recursive resolver (Unbound) as the organization's internal DNS forwarder; configure all SOHO routers to point exclusively to this internal resolver IP; Pi-hole's query log provides a single pane of glass for all DNS queries and will immediately surface any client querying an external resolver directly (indicating a re-hijacked router). (2) Router configuration integrity — write a weekly bash or PowerShell script that SSHs to each managed router, exports the running config, computes a SHA-256 hash ('sha256sum router_config.txt'), and compares it to the hash of the last known-good config; alert on any mismatch. Store known-good config hashes in a read-only location (e.g., a Git repository with protected main branch). (3) MFA enforcement — deploy Duo Security's free tier (up to 10 users) or configure TOTP-based MFA via Google Authenticator integration on VPN and any web-exposed admin interfaces that support RADIUS or SAML; for Windows RDP, enforce MFA via Azure AD Conditional Access if O365 licensing is already in place. (4) Threat intelligence integration — subscribe to CISA's free Known Exploited Vulnerabilities (KEV) catalog RSS feed and create a weekly review process to cross-reference KEV entries against the organization's SOHO router inventory and firmware versions.

Evidence: Retain for post-incident review and potential regulatory reporting: (1) All router configuration exports and DNS resolver diff outputs from Steps 1-4, organized by device and timestamp, forming a chronological record of the compromise and remediation. (2) Full authentication log exports covering the compromise window through 30 days post-remediation for all accounts identified as exposed — these constitute the evidentiary basis for determining whether any harvested credentials were successfully reused and whether breach notification obligations apply. (3) Lessons learned documentation capturing the initial detection gap (how long DNS was hijacked before discovery), the affected account population, and the three control gaps identified in this step — required for NIST IR-8 (Incident Response Plan) update and for any CISA voluntary incident reporting under the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) if the organization qualifies.

Detection Guidance

Detection requires network-layer visibility; endpoint-based AV and EDR will produce no alerts for this technique. Primary detection vectors: (1) DNS resolver audit - compare configured DNS resolver IPs on all SOHO routers against an approved resolver list; any deviation is a high-confidence indicator. (2) DNS query monitoring - deploy DNS logging at the network perimeter or via router syslog; look for queries resolving authentication endpoints (login pages, OAuth endpoints, VPN gateways) to unexpected IPs. (3) Authentication traffic analysis - monitor for HTTP 302 redirects or NTLM/Kerberos exchanges terminating at IP addresses outside known

infrastructure; flag mismatches between expected service IPs and resolved IPs. (4) Router management-plane audit - review router access logs for configuration changes, especially DNS settings modifications, from unauthorized source IPs or outside maintenance windows. (5) Credential anomalies - post-compromise, watch for valid account logins from unusual geographies or times, which may indicate harvested credential reuse. No specific IOC IPs or domains have been published in available source material as of this writing; any DNS resolver IP outside the approved baseline should be treated as a high-priority investigation target and the device isolated pending analysis.

Indicators of Compromise

Type	Value	Context	Confidence
NOTE	`No specific IOCs published`	Microsoft's April 2026 blog post and available secondary sources do not identify specific attacker-controlled DNS IPs, domains, or infrastructure indicators. Any unrecognized DNS resolver IP configured on SOHO routers should be treated as a high-priority investigation target. Monitor for IOC releases from Microsoft MSTIC and CISA.	LOW

Framework Mappings

MITRE-ATTACK

- **T1556** — Modify Authentication Process
- **T1562.001** — Disable or Modify Tools
- **T1071.001** — Web Protocols
- **T1133** — External Remote Services
- **T1040** — Network Sniffing
- **T1557** — Adversary-in-the-Middle
- **T1078** — Valid Accounts
- **T1584.002** — DNS Server
- **T1584.008** — Network Devices

NIST-800-53R5

- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **SI-4** — System Monitoring
- **SI-7** — Software, Firmware, and Information Integrity
- **AC-17** — Remote Access
- **AC-20** — Use of External Systems

- **SC-7** — Boundary Protection
- **AC-2** — Account Management
- **IA-8** — Identification and Authentication (Non-Organizational Users)
- **AT-2** — Literacy Training and Awareness

OWASP-TOP10-2021

- **A07:2021** — Identification and Authentication Failures

CIS-V8

- **6.3** — Require MFA for Externally-Exposed Applications
- **6.4** — Require MFA for Remote Network Access
- **6.5** — Require MFA for Administrative Access
- **7.3** — Perform Automated Operating System Patch Management
- **7.4** — Perform Automated Application Patch Management
- **14.2** — Train Workforce Members to Recognize Social Engineering Attacks
- **8.2** — Collect Audit Logs

SOC2-TSC

- **CC6.1** — The entity implements logical access security software, infrastructure, and architectures over protected information assets
- **CC9.2** — Manages risks associated with vendors and business partners

HIPAA-SECURITY

- **164.312(d)** — Person or Entity Authentication

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities
- **A.5.21** — Managing information security in the ICT supply chain

NIST-CSF-2

- **DE.CM-01** — Networks and network services are monitored

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1556	Modify Authentication Process	Credential-Access
T1562.001	Disable or Modify Tools	Defense-Evasion
T1071.001	Web Protocols	Command-And-Control
T1133	External Remote Services	Persistence
T1040	Network Sniffing	Credential-Access

Technique ID	Technique Name	Tactic
T1557	Adversary-in-the-Middle	Credential-Access
T1078	Valid Accounts	Defense-Evasion
T1584.002	DNS Server	Resource-Development
T1584.008	Network Devices	Resource-Development

Sources

Source	URL	Tier
Security News	https://www.darkreading.com/threat-intelligence/russia-forest-blizz...	T3
SOHO router compromise leads to DNS hijacking and ... - Microsoft	https://www.microsoft.com/en-us/security/blog/2026/04/07/soho-route...	T1
Consumer routers have had issues, but often because ... - Facebook	https://www.facebook.com/eff/posts/consumer-routers-have-had-issues...	T3
The many vulnerabilities Talos discovered in SOHO and industrial ...	https://blog.talosintelligence.com/router-researcher-vulnerability-...	T3
[PDF] SOHO Router Security - Tufts University	https://www.cs.tufts.edu/comp/116/archive/fall2014/mdavis.pdf	T1

Generated 2026-04-09 06:07 UTC by TJS Security Command Center