INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-22 13:59 UTC

Canada's Intelligence Service Remotely Disinfected Botnet-Compromised Devices Under First-Ever Threat Reduction Warrant

THREAT CAMPAIGN | HIGH | CVSS 7.5

SCC Item ID	SCC-CAM-2026-0535
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Cisco SOHO routers (end-of-life), NetGear routers (end-of-life), Ubiquiti routers, Ring doorbells, IP security cameras, IoT-enabled consumer devices (TVs, Wi-Fi appliances), Canadian-geolocated devices compromised by foreign state-linked botnet infrastructure
Published	2026-06-22T05:11:37
Discovery Source	Rss

Executive Summary

In May 2024, Canada's Security Intelligence Service executed the country's first court-authorized cyber operation to remotely remove malicious implants from Canadian-geolocated SOHO routers, servers, and IoT devices compromised by a foreign state actor. The operation, unsealed in June 2026, targeted the same device classes, end-of-life Cisco, NetGear, and Ubiquiti routers alongside consumer IoT, exploited in parallel U.S. operations against Volt Typhoon and APT28 botnet infrastructure. Organizations and households running end-of-life SOHO hardware face material risk: these devices serve as persistent, low-visibility footholds for state-linked espionage and pre-positioning activity that bypasses traditional enterprise perimeter controls.

Technical Analysis

The CSIS operation targeted botnet infrastructure embedded in end-of-life SOHO and IoT hardware across Canadian IP space. Affected device classes share a consistent vulnerability profile: insecure default configurations (CWE-1188), missing authentication for critical functions (CWE-306), hidden backdoor functionality in end-of-life firmware (CWE-912), and inadequate protection mechanisms enabling exploitation of trust relationships (CWE-693). No single CVE governs this campaign; the attack surface is the firmware lifecycle gap itself. MITRE ATT&CK techniques observed in parallel operations include T1584.005 (botnet infrastructure acquisition via compromised devices), T1583.003 (virtual private server provisioning), T1078.001 (default

account abuse), T1133 (external remote services), T1542.004 (ROMMONkit/pre-OS persistence), T1562.001 (defense evasion via security tool impairment), T1571 (non-standard port communication), T1090.003 (multi-hop proxy via compromised nodes), and T1016 (network configuration discovery). The threat actor category is unnamed foreign state actor for the Canadian operation; Volt Typhoon and APT28 are cited contextually for parallel U.S. operations. No patches are available for end-of-life hardware; replacement is the only full remediation path. The operation's legal framework raises unresolved questions regarding warrantless IP address collection during target identification and the absence of mandatory victim notification.

Action Checklist

1. Step 1: Containment, Audit all network edge devices immediately. Identify any Cisco SOHO (e.g., RV-series), NetGear, Ubiquiti routers, Ring doorbells, IP cameras, and IoT-enabled appliances that have reached end-of-life status and have no current firmware support. Isolate internet-facing end-of-life devices from sensitive network segments pending replacement. Disable remote management interfaces (telnet, HTTP, HTTPS admin) on all SOHO devices not actively requiring them. Reference CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory) to ensure full device visibility before proceeding.
2. Step 2: Detection, Query DHCP, NAT, and firewall logs for outbound connections to non-standard ports (T1571) and multi-hop proxy patterns (T1090.003) originating from SOHO or IoT device IP addresses. Review authentication logs for use of default credentials on network devices (T1078.001). Monitor DNS and NetFlow for communication patterns consistent with C2 beaconing: low-TTL resolutions, periodic outbound connections to unfamiliar external IPs, or traffic to known VPS hosting ranges. Check router syslog for unexpected configuration changes, new admin accounts, or reboots not initiated by your team. Use D3-LAM (Local Account Monitoring) to surface unauthorized local account activity on network devices where syslog is available.
3. Step 3: Eradication, For any confirmed or suspected end-of-life device, replace hardware; do not attempt firmware reimaging alone, as CWE-912 (hidden backdoor in end-of-life firmware) means implants may survive factory resets. For still-supported devices showing anomalous behavior, apply the latest available firmware from the official vendor portal, restore configuration from a known-good baseline, and rotate all device credentials (D3-CRO, Credential Rotation). Disable default accounts and rename or disable any vendor-preset administrative accounts (CIS 4.7, Manage Default Accounts on Enterprise Assets and Software). Enforce strong, unique credentials per CIS 5.2.
4. Step 4: Recovery, After replacement or remediation, validate that no unauthorized accounts remain, all management interfaces are access-controlled, and outbound traffic from the device class returns to baseline. Re-enable logging to a centralized syslog or SIEM (CIS 8.2, Collect Audit Logs; NIST AU-2, Event Logging) and confirm log ingestion is active. Monitor new device traffic for 30 days post-replacement for residual C2 patterns that may indicate lateral movement from previously compromised segments. Verify firewall rules block inbound management access from untrusted IP ranges (CIS 4.4, Implement and Manage a Firewall on Servers).
5. Step 5: Post-Incident, This campaign exposes three control gaps: (1) absence of a complete asset inventory covering network infrastructure and IoT (CIS 1.1), (2) no formal end-of-life device retirement process tied to vendor EOS announcements (CIS 2.2, Ensure Authorized Software is Currently Supported), and (3) insufficient network segmentation allowing compromised SOHO devices to pivot toward internal resources (NIST AC-4, Information Flow Enforcement). Establish a hardware lifecycle policy that mandates replacement planning at vendor EOS announcement, not after compromise. Review whether remote management is enabled on any device that does not require it, and enforce least privilege

on all network device accounts (NIST AC-6, Least Privilege).

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate immediately to senior leadership, legal counsel, and relevant national cyber authority (CISA in the U.S., CCCS in Canada) if any SOHO or IoT device is confirmed to have forwarded internal network traffic, if C2 beaconing to Volt Typhoon- or APT28-associated infrastructure is detected, or if the organization operates critical infrastructure sectors identified in CISA AA24-038A (energy, water, communications, transportation), as these conditions trigger mandatory incident reporting obligations and potential law enforcement coordination.
Recovery Notes	After replacing or remediating confirmed end-of-life Cisco RV-series, NetGear, and Ubiquiti devices, monitor all previously reachable internal network segments for 30 days using NetFlow and DNS log analysis, specifically watching for re-emergence of beaconing to VPS ASNs (Vultr, Choopa, M247) and GRE tunnel establishment documented in FBI and CISA advisories on this campaign's infrastructure. Verify that no internal hosts communicated with botnet C2 nodes during the compromise window by reviewing historical firewall and proxy logs against the IOC lists published in CISA AA24-038A and AA24-085A. Confirm that the replacement device's management interface is accessible only from a dedicated administrative VLAN and that all legacy protocols (Telnet, HTTP admin, SNMPv1/v2 with default community strings) are disabled before returning the device to production.
Forensic Artifacts	Ubiquiti EdgeRouter flash dump (`dd if=/dev/mtd0`) and `/etc/config` directory: Volt Typhoon implants documented by FBI/CISA persisted in NVRAM and modified startup scripts to survive factory reset; the flash dump preserves implant binaries and modified init scripts that are destroyed by reflashing. | Cisco RV-series (RV320/RV325) syslog buffer and running configuration export: APT28 Moobot and Volt Typhoon KV-botnet implants on these devices added unauthorized administrator accounts and persistent port-forward rules to `/etc/config/firewall`; the running config captures these additions before they are removed during eradication. | NetFlow or `tcpdump` capture from WAN interface of compromised SOHO device: this campaign's C2 traffic exhibits characteristic patterns — periodic outbound TCP connections on non-standard high ports (4443, 8443, 1080) to Vultr/Choopa/M247 ASN space and GRE encapsulation — that distinguish botnet relay traffic from legitimate user traffic and are the primary network-layer IOC for this specific campaign. | DHCP lease history and ARP cache tables from upstream network infrastructure: correlates SOHO/IoT device MAC addresses to IP assignments across the full compromise window, enabling reconstruction of which internal hosts routed traffic through the compromised device and may have been proxied to external C2 infrastructure. | Router `/var/log/messages` and authentication log (`/var/log/auth.log`) from Linux-based Ubiquiti and supported NetGear devices: contain timestamps of unauthorized SSH login events using default credentials (`ubnt`/`ubnt`, `admin`/`password`) and subsequent privilege escalation or implant installation commands, which are the primary host-layer forensic record of initial access for this campaign's intrusion methodology.

Per-Action IR Details

Step 1: Containment — Audit all network edge devices immediately. Identify any Cisco SOHO (e.g., RV-series), NetGear, Ubiquiti routers, Ring doorbells, IP cameras, and IoT-enabled appliances that have reached end-of-life status and have no current firmware support. Isolate internet-facing end-of-life devices from

sensitive network segments pending replacement. Disable remote management interfaces (telnet, HTTP, HTTPS admin) on all SOHO devices not actively requiring them. Reference CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory) to ensure full device visibility before proceeding.

NIST Phase: Containment

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

Controls: CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), NIST AC-4 (Information Flow Enforcement), CIS 4.4 (Implement and Manage a Firewall on Servers)

Compensating: Run `nmap -sV --open -p 23,80,443,8080,8443 ` to enumerate exposed management interfaces on SOHO/IoT device IPs. Cross-reference discovered devices against Cisco RV-series, NetGear, and Ubiquiti EOS lists published at cisco.com/c/en/us/products/eos-eol-policy.html and netgear.com/about/end-of-life. For segmentation without enterprise gear, configure VLAN isolation on a managed switch (e.g., Netgear GS308E using its free GUI) to quarantine flagged device subnets from internal LAN segments.

Evidence: Before isolating any device, capture: (1) full `arp -a` and `ip neigh` tables from the upstream router/switch to record MAC-to-IP mappings of all SOHO/IoT devices; (2) active SNMP walks (`snmpwalk -v2c -c public `) if SNMP is enabled, to record current running configuration state; (3) screenshot or text dump of any web-based admin console showing current firmware version, active admin accounts, and NAT/port-forward rules — Volt Typhoon and APT28 implants targeting Cisco RV-series and Ubiquiti EdgeRouters have been observed adding unauthorized port-forward rules and admin accounts that disappear after power cycle.

Step 2: Detection — Query DHCP, NAT, and firewall logs for outbound connections to non-standard ports (T1571) and multi-hop proxy patterns (T1090.003) originating from SOHO or IoT device IP addresses. Review authentication logs for use of default credentials on network devices (T1078.001). Monitor DNS and NetFlow for communication patterns consistent with C2 beaconing: low-TTL resolutions, periodic outbound connections to unfamiliar external IPs, or traffic to known VPS hosting ranges. Check router syslog for unexpected configuration changes, new admin accounts, or reboots not initiated by your team. Use D3-LAM (Local Account Monitoring) to surface unauthorized local account activity on network devices where syslog is available.

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), CIS 8.2 (Collect Audit Logs)

Compensating: Without SIEM, forward Cisco RV-series and Ubiquiti syslog to a free Graylog or Syslog-NG instance on an internal Linux host (`rsyslog` with `*.* @:514` in `/etc/rsyslog.conf` on supported devices). Use `ntopng` (community edition) or `tcpdump -i -w /tmp/capture.pcap` on a mirrored WAN port to capture NetFlow-equivalent data. Apply the public Sigma rule `net_connection_lolbas.yml` adapted for router syslog to flag outbound connections on ports 443/8443/4443/1080 from device IPs. For DNS beaconing, run `zeek` on a span port and query `dns.log` for TTL values under 300 seconds resolving to ASNs associated with Vultr, Choopa, or M247 — VPS providers documented in FBI and CISA advisories on Volt Typhoon and APT28 SOHO botnet infrastructure.

Evidence: This step is analytical and does not alter live state. Preserve before beginning analysis: (1) raw syslog from all Cisco RV-series, NetGear, and Ubiquiti devices covering at minimum 90 days — implants associated with this campaign have shown dwell times exceeding 180 days; (2) DHCP lease history from the upstream router or Windows DHCP server (`Get-DhcpServerv4Lease -ScopeId ` on Windows Server) to correlate device IPs across the compromise window; (3) firewall/NAT rule tables exported to file before any changes — Volt Typhoon-linked implants on Cisco RV320/RV325 and Ubiquiti EdgeRouters were documented by FBI and CISA (AA24-038A) as adding persistent port-forward rules and GRE tunnels that survive reboots via modified `/etc/config` or NVRAM writes.

Step 3: Eradication — For any confirmed or suspected end-of-life device, replace hardware; do not attempt firmware reimaging alone, as CWE-912 (hidden backdoor in end-of-life firmware) means implants may survive factory resets. For still-supported devices showing anomalous behavior, apply the latest available firmware from the official vendor portal, restore configuration from a known-good baseline, and rotate all device

credentials (D3-CRO — Credential Rotation). Disable default accounts and rename or disable any vendor-preset administrative accounts (CIS 4.7 — Manage Default Accounts on Enterprise Assets and Software). Enforce strong, unique credentials per CIS 5.2.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: CIS 4.7 (Manage Default Accounts on Enterprise Assets and Software), CIS 5.2 (Use Unique Passwords), CIS 2.2 (Ensure Authorized Software is Currently Supported)

Compensating: For Ubiquiti EdgeRouter devices still in support, use the official CLI: `add system image ` followed by `reboot` into the new image, then `delete system image` for the old version. Restore config from a pre-compromise baseline using `scp baseline.tar.gz admin@:/tmp/` and `restore-config /tmp/baseline.tar.gz`. For NetGear devices still in support, download firmware directly from netgear.com/support/download and perform manual TFTP flash. For all devices post-remediation, use `passwd` (Linux-based routers) or device-specific CLI to set unique 16+ character credentials and disable the `admin`/`ubnt`/`root` default accounts documented in CISA advisory AA24-038A as entry vectors for this campaign.

Evidence: CRITICAL — volatile capture MUST precede any firmware flash, factory reset, or hardware replacement: (1) acquire a full flash dump if technically feasible using `dd if=/dev/mtd0 of=/tmp/flash_dump.bin` (Ubiquiti EdgeRouter via SSH) or equivalent — implant binaries on Ubiquiti and Cisco RV-series devices in this campaign persisted in non-volatile storage regions not cleared by factory reset; (2) export running configuration (`show running-config` on Cisco RV-series, `show configuration` on Ubiquiti) to a forensic copy; (3) collect `/var/log/messages` and `/tmp/system.log` from Ubiquiti devices and the equivalent syslog buffer from Cisco RV-series before power cycle — these logs contain implant installation timestamps and C2 connection history that are lost on reboot; (4) photograph or screenshot all active port-forwarding, firewall, and admin account settings as chain-of-custody documentation aligned with NIST 800-61r3 §3.4 evidence preservation guidance.

Step 4: Recovery — After replacement or remediation, validate that no unauthorized accounts remain, all management interfaces are access-controlled, and outbound traffic from the device class returns to baseline. Re-enable logging to a centralized syslog or SIEM (CIS 8.2 — Collect Audit Logs; NIST AU-2 — Event Logging) and confirm log ingestion is active. Monitor new device traffic for 30 days post-replacement for residual C2 patterns that may indicate lateral movement from previously compromised segments. Verify firewall rules block inbound management access from untrusted IP ranges (CIS 4.4 — Implement and Manage a Firewall on Servers).

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: CIS 8.2 (Collect Audit Logs), NIST AU-2 (Event Logging), CIS 4.4 (Implement and Manage a Firewall on Servers), NIST AC-17 (Remote Access)

Compensating: Validate account hygiene with a post-replacement config audit script: on Ubiquiti EdgeRouter, `cat /etc/passwd | grep -v nologin` to confirm no residual implant-added accounts; on Cisco RV-series, `show ip ssh` and `show users` via serial console. Establish a baseline traffic profile by running `ntopng` or `iftop` on the WAN interface for 72 hours post-replacement and flag any outbound connections to ASNs not present in the pre-compromise baseline. Set a cron job (`0 * * * * netstat -an | grep ESTABLISHED >> /var/log/conn_audit.log`) on Linux-based replacement devices to capture hourly connection snapshots during the 30-day watch period. Confirm syslog forwarding is active by sending a test message (`logger -p local0.info 'GAIO-TEST'`) and verifying receipt at the syslog server.

Evidence: This step follows eradication; volatile evidence should already be preserved. However, during the 30-day monitoring window, retain: (1) all NetFlow or connection logs from the new device's WAN interface — if internal hosts that previously communicated through the compromised SOHO device initiate outbound connections to the same C2 IP ranges documented in CISA AA24-038A (Volt Typhoon) or AA24-085A (APT28 botnet), this indicates the implant achieved lateral movement before containment; (2) DNS query logs from the new device or upstream resolver, specifically monitoring for re-resolution of domains previously associated with the botnet's KV-botnet or Moobot C2 infrastructure; (3) authentication logs (`/var/log/auth.log` or Windows Security Event ID 4624/4625) on internal servers

that were reachable from the previously compromised SOHO segment.

Step 5: Post-Incident — This campaign exposes three control gaps: (1) absence of a complete asset inventory covering network infrastructure and IoT (CIS 1.1), (2) no formal end-of-life device retirement process tied to vendor EOS announcements (CIS 2.2 — Ensure Authorized Software is Currently Supported), and (3) insufficient network segmentation allowing compromised SOHO devices to pivot toward internal resources (NIST AC-4 — Information Flow Enforcement). Establish a hardware lifecycle policy that mandates replacement planning at vendor EOS announcement, not after compromise. Review whether remote management is enabled on any device that does not require it, and enforce least privilege on all network device accounts (NIST AC-6 — Least Privilege).

NIST Phase: Post Incident

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

Controls: CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 2.2 (Ensure Authorized Software is Currently Supported), NIST AC-4 (Information Flow Enforcement), NIST AC-6 (Least Privilege)

Compensating: Establish a no-cost EOS tracking process: subscribe to Cisco PSIRT (tools.cisco.com/security/center/psirt), NetGear security advisories (netgear.com/about/security), and Ubiquiti community release notes via RSS. Maintain the asset inventory in a shared spreadsheet or free Snipe-IT instance with a calculated 'Days to EOS' column auto-flagging devices within 180 days of vendor end-of-support. For segmentation without enterprise firewalls, implement ACLs on managed switches to deny SOHO/IoT device subnets from reaching internal server VLANs, using the free GNS3 or pfSense (open source) as a segmentation gateway. Document lessons learned using the CISA SOHO Router Security Guide (published post-Volt Typhoon disclosures) as a benchmark for policy gaps.

Evidence: Post-incident artifact preservation for lessons learned and potential law enforcement referral: (1) retain all flash dumps, configuration exports, and syslog captures collected during Steps 2–4 for a minimum of 12 months in write-once storage — CISA's unsealed warrant documentation from the Canadian CSIS operation indicates these artifacts constitute evidence of a foreign state-sponsored intrusion and may be subject to legal hold; (2) document the full device inventory with MAC addresses, firmware versions at time of discovery, and EOS dates — this data directly supports a criminal referral to RCMP or CSIS under Canada's CSIS Act if Canadian-geolocated devices are involved, or to CISA/FBI under U.S. 18 U.S.C. § 1030 if applicable; (3) retain NetFlow and DNS logs showing C2 beaconing patterns for submission to CISA's MIFR (Malware Initial Findings Report) process or sharing via AIS (Automated Indicator Sharing) to contribute to collective defense against this ongoing campaign.

Detection Guidance

Focus detection on behavioral anomalies from SOHO router and IoT device IP ranges rather than signature-based indicators, as no public IOC list has been released for the Canadian operation. Key detection approaches: (1) NetFlow or firewall log analysis, flag sustained outbound sessions from router management IPs to external hosts, especially on non-standard ports per T1571; (2) DNS query logs, identify SOHO device IPs initiating DNS lookups not consistent with normal NTP, update, or management traffic; (3) Authentication logs, alert on successful logins to router admin interfaces using default usernames (admin, root, cisco, netgear) per T1078.001; (4) Syslog from managed devices, parse for unexpected configuration writes, privilege escalation events, or new user creation not tied to a change ticket; (5) Outbound proxy-chain patterns, traffic from internal devices routing through an intermediate SOHO device to external VPS infrastructure is a strong behavioral indicator of T1090.003 and T1583.003. D3-SFA (System File Analysis) applies where device file systems are accessible for integrity checks. D3-LAM (Local Account Monitoring) applies on devices with accessible account databases. Absence of logging on end-of-life devices is itself a detection gap, CIS 8.2 and NIST AU-2 compliance requires that all network devices capable of logging are enrolled in centralized log collection.

Indicators of Compromise

Type	Value	Context	Confidence
IP	`not-published`	No IOCs from the CSIS operation have been released in the public record as of the unsealing date. The upstream pipeline has found no actionable IOC list associated with this campaign.	LOW

Framework Mappings

MITRE-ATTACK

- **T1571** — Non-Standard Port
- **T1584.005** — Botnet
- **T1583.003** — Virtual Private Server
- **T1078.001** — Default Accounts
- **T1016** — System Network Configuration Discovery
- **T1133** — External Remote Services
- **T1542.004** — ROMMONkit
- **T1562.001** — Disable or Modify Tools
- **T1090.003** — Multi-hop Proxy

NIST-800-53R5

- **AC-17** — Remote Access
- **AC-20** — Use of External Systems
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **SC-7** — Boundary Protection

OWASP-TOP10-2021

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

CIS-V8

- **6.3** — Require MFA for Externally-Exposed Applications

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1571	Non-Standard Port	Command-And-Control
T1584.005	Botnet	Resource-Development
T1583.003	Virtual Private Server	Resource-Development
T1078.001	Default Accounts	Defense-Evasion
T1016	System Network Configuration Discovery	Discovery
T1133	External Remote Services	Persistence
T1542.004	ROMMONkit	Defense-Evasion
T1562.001	Disable or Modify Tools	Defense-Evasion
T1090.003	Multi-hop Proxy	Command-And-Control

Sources

Source	URL	Tier
Security News	https://thehackernews.com/2026/06/canadas-spy-agency-used-first-of-...	T3
How does End of Life/Outdated firmware suddenly become an issue ...	https://www.reddit.com/r/networking/comments/128k66s/how_does_end_o...	T3
End of Service Products - Netgear	https://www.netgear.com/about/eos/	T3
Forced to buy new router after 6 years - Facebook	https://www.facebook.com/groups/372119787729533/posts/1266404774967...	T3
Router Support Ending [US restrictions for new router purchases]	https://www.bogleheads.org/forum/viewtopic.php?t=467719	T3

Generated 2026-06-22 13:59 UTC by TJS Security Command Center