Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

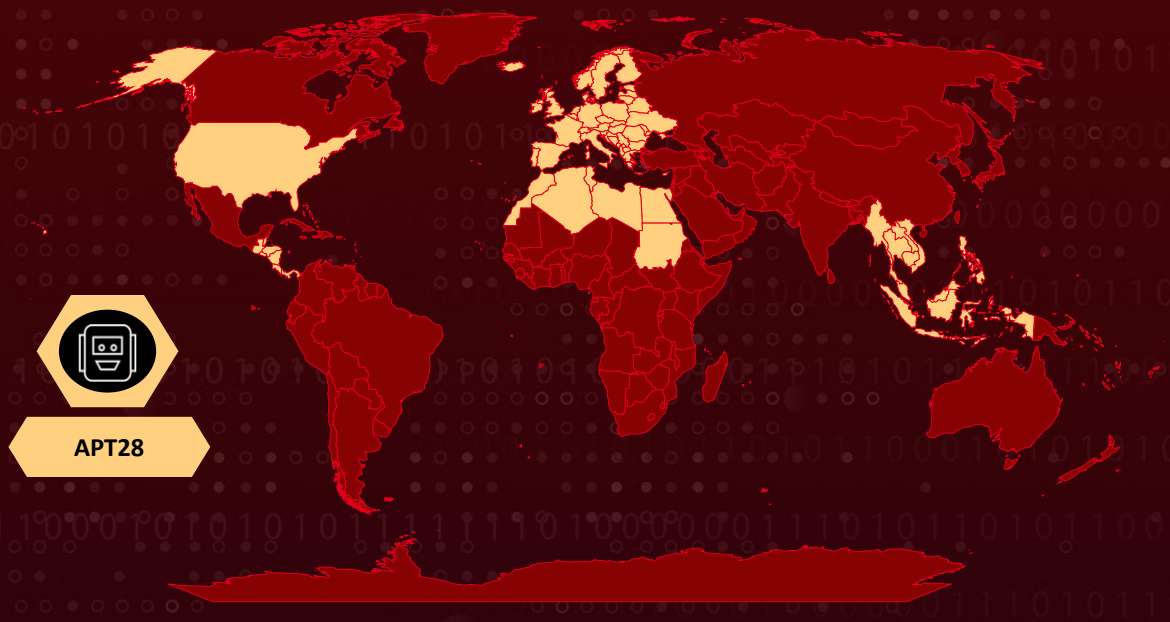
APT28 Exploits SOHO Routers for Large-Scale DNS Hijacking and Credential Theft

Date of Publication	Admiralty Code	TA Number
April 09, 2026	A1	TA2026093

Summary

First Seen: May 2025
Targeted Regions: North Africa, Central America, Southeast Asia, Europe, Ukraine, United States
Targeted Platforms: SOHO Routers (TP-Link, MikroTik), Windows Endpoints, Microsoft 365/ Outlook on the Web
Targeted Industries: Government, Critical Infrastructure, Information Technology, Telecommunications, Energy, Third-party Email and Cloud Service Providers
Campaign Name: FrostArmada
Threat Actor: APT28 (aka Sofacy, Fancy Bear, Sednit, Group 74, TG-4127, Pawn Storm, Tsar Team, Strontium, Swallowtail, SIG40, Snakemackerel, Iron Twilight, ATK 5, T-APT-12, ITG05, TAG-0700, UAC-0028, FROZENLAKE, Grey-Cloud, Forest Blizzard, GruesomeLarch, BlueDelta, TA422, Fighting Ursa, Blue Athena, UAC-0063, TAG-110)
Attack: APT28, operating under Russia's GRU Military Unit 26165, conducted a large-scale DNS hijacking campaign by exploiting known vulnerabilities in SOHO routers, primarily TP-Link and MikroTik devices. The actors modified DHCP/DNS settings on compromised routers to redirect DNS requests to attacker-controlled servers. For targets of intelligence value, these malicious DNS resolvers returned spoofed DNS records for domains associated with web-based email services and other login portals, enabling adversary-in-the-middle (AitM) attacks on TLS connections. This allowed the actors to harvest unencrypted passwords, OAuth authentication tokens, emails, and other sensitive data from downstream devices without deploying any malware. At peak activity in December 2025, over 18,000 unique IP addresses across 120+ countries were communicating with APT28 infrastructure, with an estimated 200+ organizations and 5,000 consumer devices impacted.

Attack Regions



CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2023-50224	TP-Link TL-WR841N Authentication Bypass by Spoofing Vulnerability	TP-Link WR841N	✗	✓	✓

Attack Details

#1

APT28, the Russian state-sponsored threat group operating under GRU Military Intelligence Unit 26165, has been conducting a large-scale cyber espionage campaign targeting small office and home office (SOHO) routers, primarily MikroTik and TP-Link devices, to build a distributed DNS hijacking infrastructure. Tracked under the name FrostArmada by researchers, the operation began in limited form around May 2025, escalated significantly by August, and reached its peak in December 2025, at which point over 18,000 unique IP addresses across more than 120 countries were communicating with attacker-controlled infrastructure.

#2

The attack chain began with APT28 gaining remote administrative access to vulnerable routers, notably exploiting CVE-2023-50224 on TP-Link WR841N devices, an authentication bypass flaw that allowed credential extraction through crafted HTTP requests. Once inside, the attackers reconfigured the router's DHCP and DNS settings to point to malicious virtual private servers acting as DNS resolvers. These poisoned settings were then automatically propagated to every device on the local network via DHCP, meaning end users required no interaction to become victims. The technique was nearly invisible, the only telltale sign was an invalid TLS certificate warning that most users would dismiss.

#3

When users on compromised networks attempted to access targeted domains, particularly web-based email portals and other authentication services, the malicious DNS servers resolved those requests to attacker-in-the-middle nodes. At these nodes, APT28 harvested usernames, passwords, and OAuth tokens in real time. The operation was structured into two distinct clusters: an expansion team focused on compromising new devices and growing the botnet, and a second team dedicated to credential interception and exfiltration operations.

#4 The campaign's targeting was broad but strategically filtered. APT28 cast a wide net across government agencies, ministries of foreign affairs, law enforcement bodies, and third-party email and cloud providers in North Africa, Central America, Southeast Asia, and Europe. Over 200 organizations and 5,000 consumer devices were estimated to have been impacted. The opportunistic initial compromise allowed the actors to identify high-value intelligence targets and progressively narrow their focus at each successive stage of the exploitation chain.

#5 An international law enforcement effort, designated Operation Masquerade, has now disrupted the campaign. Authorities executed a court-authorized technical operation to reset DNS configurations on compromised routers, restoring them to legitimate resolvers. Defenders are advised to implement certificate pinning on managed devices, aggressively patch router firmware, minimize internet-facing exposure of network equipment, and retire any end-of-life hardware.

Recommendations

Verify and Secure Router DNS Settings: Immediately audit DNS configurations on all SOHO routers across the organization. Ensure primary and secondary DNS resolvers point to legitimate servers provided by your ISP or trusted DNS providers. Establish a baseline and monitor for unauthorized changes to DHCP and DNS settings on a regular basis.

Patch Firmware and Replace End-of-Life Devices: Apply the latest firmware updates to all MikroTik, TP-Link, and other edge devices to remediate known vulnerabilities like CVE-2023-50224. Identify and decommission any end-of-life routers that no longer receive security updates, as these remain permanently exploitable entry points into the network.

Implement Certificate Pinning on Managed Devices: Deploy certificate pinning policies through your MDM solution for all corporate laptops, phones, and tablets. This ensures that when an attacker attempts to intercept TLS connections through a rogue DNS resolver, the device will reject the fraudulent certificate rather than silently connecting to malicious infrastructure.

Restrict Remote Administration on Edge Devices: Disable remote management interfaces on routers and firewalls unless absolutely necessary. Where remote access is required, enforce strong authentication, restrict access to trusted IP ranges, and use VPN tunnels. Publicly exposed admin panels are the primary vector APT28 used to compromise devices at scale.

Monitor DNS Traffic for Anomalous Activity: Deploy DNS logging and monitoring across the network to detect unusual query patterns, unexpected resolver changes, or traffic flowing to unfamiliar IP addresses. Maintain blocklists of known malicious domains and IPs published in the indicators of compromise, and integrate DNS telemetry into your SIEM for real-time alerting.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	T1190: Exploit Public-Facing Application	
	T1078: Valid Accounts	
Resource Development	T1583: Acquire Infrastructure	T1583.002: DNS Server
		T1583.003: Virtual Private Server
	T1588: Obtain Capabilities	T1588.006: Vulnerabilities
	T1586: Compromise Accounts	
Credential Access	T1528: Steal Application Access Token	
	T1556: Modify Authentication Process	
Collection	T1557: Adversary-in-the-Middle	
Persistence	T1584: Compromise Infrastructure	T1584.008: Network Devices
Reconnaissance	T1595: Active Scanning	
Command and Control	T1071: Application Layer Protocol	T1071.004: DNS
Defense Evasion	T1036: Masquerading	

Indicators of Compromise (IOCs)

TYPE	VALUE
Domains	autodiscover-s[.]outlook[.]com, imap-mail[.]outlook[.]com, outlook[.]live[.]com, outlook[.]office[.]com, outlook[.]office365[.]com
VPS Banner Pattern	SSH on TCP port 56777, dnsmasq-2.85 on UDP port 53, SSH on TCP port 35681, dnsmasq-2.85 on UDP port 53
IPv4	5[.]226[.]137[.]151, 5[.]226[.]137[.]230, 5[.]226[.]137[.]231, 5[.]226[.]137[.]232, 5[.]226[.]137[.]234, 5[.]226[.]137[.]235, 5[.]226[.]137[.]242, 5[.]226[.]137[.]243, 5[.]226[.]137[.]244, 5[.]226[.]137[.]245, 23[.]106[.]120[.]119, 37[.]221[.]64[.]77, 37[.]221[.]64[.]78, 37[.]221[.]64[.]93, 37[.]221[.]64[.]101, 37[.]221[.]64[.]116, 37[.]221[.]64[.]131, 37[.]221[.]64[.]148, 37[.]221[.]64[.]149, 37[.]221[.]64[.]150, 37[.]221[.]64[.]151, 37[.]221[.]64[.]163, 37[.]221[.]64[.]173, 37[.]221[.]64[.]199

TYPE	VALUE
IPv4	37[.]221[.]64[.]208, 37[.]221[.]64[.]224, 37[.]221[.]64[.]254, 64[.]120[.]31[.]96, 64[.]120[.]31[.]97, 64[.]120[.]31[.]98, 64[.]120[.]31[.]99, 64[.]120[.]31[.]100, 77[.]83[.]197[.]37, 77[.]83[.]197[.]38, 77[.]83[.]197[.]39, 77[.]83[.]197[.]40, 77[.]83[.]197[.]41, 77[.]83[.]197[.]42, 77[.]83[.]197[.]43, 77[.]83[.]197[.]44, 77[.]83[.]197[.]45, 77[.]83[.]197[.]46, 77[.]83[.]197[.]47, 77[.]83[.]197[.]48, 77[.]83[.]197[.]49, 77[.]83[.]197[.]50, 77[.]83[.]197[.]51, 77[.]83[.]197[.]52, 77[.]83[.]197[.]53, 77[.]83[.]197[.]54, 77[.]83[.]197[.]55, 77[.]83[.]197[.]56, 77[.]83[.]197[.]57, 77[.]83[.]197[.]58, 77[.]83[.]197[.]59, 77[.]83[.]197[.]60, 79[.]141[.]160[.]78, 79[.]141[.]161[.]66, 79[.]141[.]161[.]67, 79[.]141[.]161[.]68, 79[.]141[.]161[.]69, 79[.]141[.]161[.]70, 79[.]141[.]161[.]71,

TYPE	VALUE
IPv4	79[.]141[.]161[.]72, 79[.]141[.]161[.]73, 79[.]141[.]161[.]74, 79[.]141[.]161[.]75, 79[.]141[.]161[.]76, 79[.]141[.]161[.]77, 79[.]141[.]161[.]78, 79[.]141[.]161[.]79, 79[.]141[.]161[.]80, 79[.]141[.]161[.]81, 79[.]141[.]161[.]82, 79[.]141[.]161[.]83, 79[.]141[.]161[.]84, 79[.]141[.]161[.]85, 79[.]141[.]173[.]70, 79[.]141[.]173[.]96, 79[.]141[.]173[.]97, 79[.]141[.]173[.]98, 79[.]141[.]173[.]103, 79[.]141[.]173[.]119, 79[.]141[.]173[.]120, 79[.]141[.]173[.]121, 79[.]141[.]173[.]122, 79[.]141[.]173[.]211, 79[.]141[.]173[.]231, 79[.]141[.]173[.]232, 79[.]141[.]173[.]233, 185[.]117[.]88[.]22, 185[.]117[.]88[.]28, 185[.]117[.]88[.]29, 185[.]117[.]88[.]30, 185[.]117[.]88[.]31, 185[.]117[.]88[.]50, 185[.]117[.]88[.]60, 185[.]117[.]88[.]61, 185[.]117[.]88[.]62, 185[.]117[.]89[.]32, 185[.]117[.]89[.]46, 185[.]117[.]89[.]47,

TYPE	VALUE
IPv4	185[.]237[.]166[.]55, 185[.]237[.]166[.]56, 185[.]237[.]166[.]57, 185[.]237[.]166[.]58, 185[.]237[.]166[.]59, 185[.]237[.]166[.]60, 185[.]237[.]166[.]61, 185[.]237[.]166[.]62, 185[.]237[.]166[.]63, 185[.]237[.]166[.]64, 185[.]237[.]166[.]65, 185[.]237[.]166[.]66, 185[.]237[.]166[.]67, 185[.]237[.]166[.]68, 185[.]237[.]166[.]69, 185[.]237[.]166[.]70, 185[.]237[.]166[.]71, 185[.]237[.]166[.]72, 185[.]237[.]166[.]73, 185[.]237[.]166[.]74, 185[.]237[.]166[.]75, 185[.]237[.]166[.]224, 185[.]237[.]166[.]225, 185[.]237[.]166[.]226, 185[.]237[.]166[.]227, 185[.]237[.]166[.]228, 185[.]237[.]166[.]229, 185[.]237[.]166[.]230, 185[.]237[.]166[.]231, 185[.]237[.]166[.]232, 185[.]237[.]166[.]233, 185[.]237[.]166[.]234, 185[.]237[.]166[.]235, 185[.]237[.]166[.]236, 185[.]237[.]166[.]237, 185[.]237[.]166[.]238, 185[.]237[.]166[.]239, 185[.]237[.]166[.]240, 185[.]237[.]166[.]241,

TYPE	VALUE
IPv4	185[.]237[.]166[.]242, 185[.]237[.]166[.]243, 185[.]237[.]166[.]244, 185[.]237[.]166[.]245, 185[.]237[.]166[.]246, 185[.]237[.]166[.]247, 185[.]237[.]166[.]248, 185[.]237[.]166[.]249 64[.]44[.]154[.]227, 64[.]44[.]154[.]237, 64[.]44[.]154[.]238, 64[.]44[.]154[.]239, 64[.]44[.]154[.]240, 77[.]83[.]198[.]39, 79[.]141[.]173[.]123, 79[.]141[.]173[.]200, 79[.]141[.]173[.]210, 79[.]141[.]173[.]246, 79[.]141[.]173[.]247, 79[.]141[.]173[.]248, 79[.]141[.]173[.]249, 79[.]141[.]173[.]250, 79[.]141[.]173[.]251, 79[.]141[.]173[.]252, 79[.]141[.]173[.]253, 79[.]141[.]173[.]254, 79[.]143[.]87[.]229, 79[.]143[.]87[.]232, 79[.]143[.]87[.]240, 79[.]143[.]87[.]243, 79[.]143[.]87[.]249, 88[.]80[.]148[.]49, 88[.]80[.]148[.]53, 89[.]150[.]40[.]43, 89[.]150[.]40[.]86, 103[.]140[.]186[.]148, 103[.]140[.]186[.]149, 103[.]140[.]186[.]155, 185[.]234[.]73[.]58, 185[.]234[.]73[.]61, 185[.]234[.]73[.]62

Patch Link

https://www.tp-link.com/en/support/download/tl-wr841n/v12/#Firmware

References

https://www.justice.gov/opa/pr/justice-department-conducts-court-authorized-disruption-dns-hijacking-network-controlled

https://www.infosectoday.io/russian-state-linked-apt28-exploits-soho-routers-in-global-dns-hijacking-campaign/

https://www.ncsc.gov.uk/news/apt28-exploit-routers-to-enable-dns-hijacking-operations

https://krebsonsecurity.com/2026/04/russia-hacked-routers-to-steal-microsoft-office-tokens/

https://www.microsoft.com/en-us/security/blog/2026/04/07/soho-router-compromise-leads-to-dns-hijacking-and-adversary-in-the-middle-attacks/

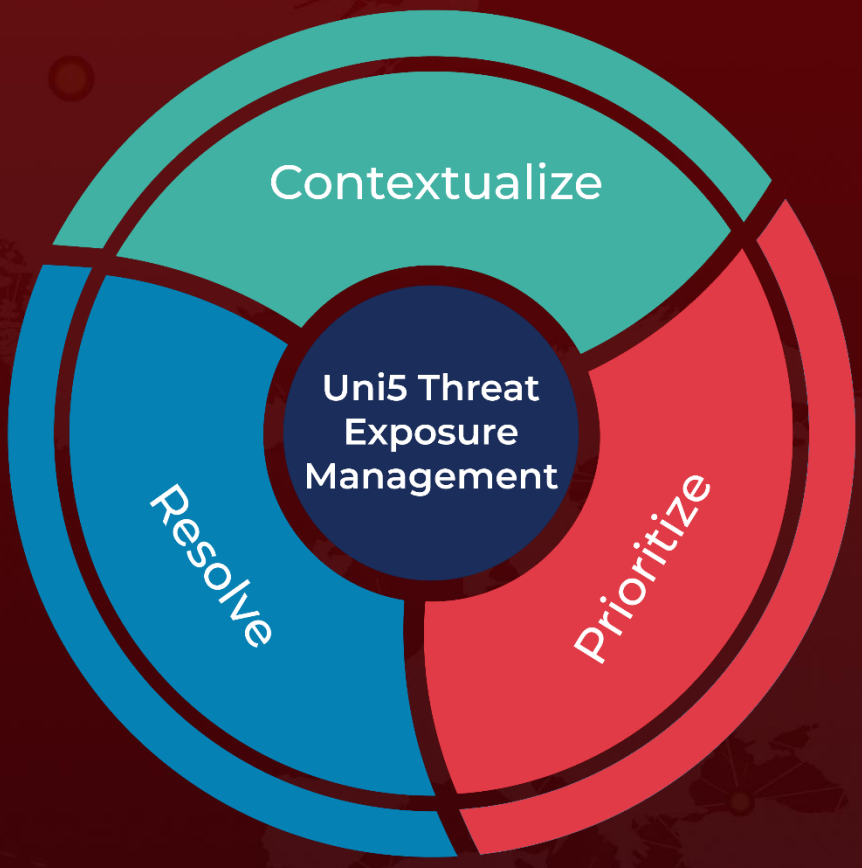
https://www.lumen.com/blog-and-news/en-us/frostarmada-forest-blizzard-dns-hijacking

https://hivepro.com/threat-advisory/tp-link-router-end-of-service-models-exploited-in-botnet-operation/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

April 09, 2026 • 07:30 AM

More at www.hivepro.com