ADVISORY FOR ICM SECTOR

APT28 Exploiting Vulnerable Routers for DNS Hijacking and Adversary-in-the-Middle Attacks

Original report published on: 8 April 2026

Classification: TLP:CLEAR

Executive Summary

On 7 April 2026, the United Kingdom's National Cyber Security Centre (NCSC), together with international partners, Federal Bureau of Investigation (FBI), and the Cybersecurity and Infrastructure Security Agency (CISA), published an advisory regarding cyber espionage activities conducted by the Nation state-sponsored threat actor APT28 (also known as Fancy Bear, Forest Blizzard, and Sofacy). The campaign involves the exploitation of vulnerable internet-facing routers to conduct Domain Name System (DNS) hijacking operations that enable Adversary-in-the-Middle (AitM) attacks against targeted users. The activity primarily targets authentication workflows associated with Microsoft 365, Outlook Web Access, and other cloud-based services.

Reportedly, APT28 compromises vulnerable TP-Link routers (likely via CVE-2023-50224), modified DHCP and DNS configurations to redirect victim traffic through attacker-controlled DNS infrastructure. This enabled the interception of authentication traffic and theft of usernames, passwords, OAuth tokens, session cookies, and other authentication artefacts. Microsoft assessed that the activity has been ongoing since at least 2025 and affected more than 200 organisations, approximately 5,000 devices globally and various sectors including Telecommunications, government, and technology.

Background

Historically, APT28 conducted cyber espionage operations against government, military, telecommunications, and critical infrastructure targets.

This operation abuse compromised routers to manipulate DNS resolution processes. By altering router DHCP/DNS configurations via specially crafted HTTP GET request, devices connected behind the affected routers automatically use attacker-controlled DNS servers, without requiring any user interaction. When users subsequently access targeted services such as Microsoft Outlook, Microsoft 365, or other authentication portals, the malicious DNS infrastructure selectively redirects those requests to attacker-controlled systems capable of conducting Adversary-in-the-Middle attacks. The threat actor then harvest authentication credentials, session cookies, OAuth tokens, and other authentication details.

Detection and Mitigation

IMDA recommend organisations to perform continual testing and validation of existing security controls to ensure detection and prevention against the APT28-related activities identified in this advisory:

- Scan for Indicators of Compromise to detect threat activities (Annex A)
- Refer to the MITRE ATT&CK techniques documented in this advisory (Annex B):
  - Create, test and validate detection rules against the threat behaviours.
  - Review DNS and DHCP configurations on routers and network appliances for unauthorised modifications.
  - Monitor for abnormal OAuth token activity, suspicious session reuse, and impossible-travel authentication events.
  - Restrict or disable internet-facing router administration interfaces, where possible.
  - Implement phishing-resistant MFA methods (FIDO2)
  - Review Microsoft 365 sign-in logs for anomalous access patterns.
  - Monitor for suspicious DNS server changes and unexpected certificate warnings.
  - Ensure timely patching of routers, firewalls, and internet-facing edge devices
  - Restrict management access using IP allowlists and VPN controls.
  - Enhance user awareness regarding redirects phishing, suspicious authentication prompts, and unexpected login notifications

Annex A – Indicators of Compromise

Domain Name	Description
autodiscover-s.outlook[.]com	Domain names targeted by APT28 for redirection to AitM infrastructure
imap-mail.outlook[.]com	

outlook.live[.]com	
outlook.office[.]com	
outlook.office365[.]com	

IP Address	Description
103.140.186[.]148	Malicious APT28 DNS servers and AitM infrastructure
103.140.186[.]149	
103.140.186[.]155	
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	
185.234.73[.]58	
185.234.73[.]61	
185.234.73[.]62	
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	
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	
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	
23.106.120[.]119	
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	
37.221.64[.]208	
37.221.64[.]224	
37.221.64[.]254	
37.221.64[.]77	
37.221.64[.]78	

37.221.64[.]93	
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	
64.120.31[.]100	
64.120.31[.]96	
64.120.31[.]97	
64.120.31[.]98	
64.120.31[.]99	
64.44.154[.]227	
64.44.154[.]237	
64.44.154[.]238	
64.44.154[.]239	
64.44.154[.]240	
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	
77.83.198[.]39	
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	
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[.]103	
79.141.173[.]119	
79.141.173[.]120	
79.141.173[.]121	
79.141.173[.]122	
79.141.173[.]123	
79.141.173[.]200	
79.141.173[.]210	
79.141.173[.]211	
79.141.173[.]231	
79.141.173[.]232	
79.141.173[.]233	
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	
79.141.173[.]70	
79.141.173[.]96	
79.141.173[.]97	
79.141.173[.]98	
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	

Annex B – MITRE ATT&CK Mapping

ATT&CK Tactic	ATT&CK ID	Technique	Observed Activity
Initial Access	T1190	Exploit Public-Facing Application	Exploitation of vulnerable internet-facing routers to gain initial access.
Resource Development	T1583.002	Acquire Infrastructure: DNS Server	Deployment of attacker-controlled DNS servers to support DNS hijacking operations.
Resource Development	T1583.003	Acquire Infrastructure: Virtual Private Server	Use of VPS infrastructure to host malicious DNS resolvers and supporting infrastructure.
Resource Development	T1584.008	Compromise Infrastructure: Network Devices	Compromise of TP-Link and MikroTik routers to facilitate DNS hijacking activities.
Credential Access	T1557	Adversary-in-the-Middle (AiTM)	Interception of authentication traffic to harvest passwords, session cookies, OAuth tokens and other credentials.

Credential Access	T1528	Steal Application Access Token	Harvesting OAuth and authentication tokens associated with Microsoft 365 and cloud services.
Collection	T1539	Steal Web Session Cookie	Theft of session cookies to facilitate account compromise and session hijacking.
Collection	T1114	Email Collection	Collection of email authentication traffic and potentially email contents.

References

- APT28 Exploit Routers to Enable DNS Hijacking Operations
- Exploitation of Vulnerable Routers to Steal Credentials
- UK Exposes State Nation Military Intelligence Hijacking Vulnerable Routers for Cyber Attacks
- APT28 DNS Hijacking and Router Exploitation Analysis