Alert: I-260407-PSA | 07 APRIL 2026

Russian GRU Exploiting Vulnerable Routers to Steal Sensitive Information

Russian General Staff Main Intelligence Directorate (GRU) cyber actors are exploiting vulnerable routers worldwide to intercept and steal sensitive military, government, and critical infrastructure information. The U.S. Department of Justice and the FBI recently disrupted a GRU network of compromised small-office home-office (SOHO) routers used to facilitate malicious DNS hijacking operations. The FBI and the following

partners are releasing this announcement to warn the public and encourage network defenders and device owners to take actions to remediate and reduce the attack surface of similar edge devices: U.S. National Security Agency (NSA) and international partners from Canada, Czech Republic, Denmark, Estonia, Finland, Germany, Italy, Latvia, Lithuania, Norway, Poland, Portugal, Romania, Slovakia, and Ukraine.

Understanding the DNS Hijacking Operations

Since at least 2024, Russian GRU 85th Main Special Service Center (85th GTsSS) cyber actors – also known as APT28, Fancy Bear, and Forest Blizzard – have been collecting credentials and exploiting vulnerable routers worldwide, including compromising TP-Link routers using CVE-2023-50224. The GRU actors changed the devices' dynamic host configuration protocol (DHCP) / domain name system (DNS) settings to introduce actor-controlled DNS resolvers. Connected devices, including laptops and phones, inherit these modified settings. The actor-controlled infrastructure resolves and captures lookups for all domain names. The GRU provides fraudulent DNS answers for specific domains and services – including Microsoft Outlook Web Access – enabling adversary-in-the-middle (AitM) attacks against encrypted traffic if users navigate through a certificate error warning. These AitM attacks would allow the actors to see the traffic unencrypted.

The GRU has harvested passwords, authentication tokens, and sensitive information including emails and web browsing information normally protected by secure socket layer (SSL) and transport layer security (TLS) encryption. The GRU has indiscriminately compromised a wide pool of U.S. and global victims and then filtered down impacted users, especially targeting information related to military, government, and critical infrastructure.

Tips to Protect Yourself

The FBI and partners have released relevant guidance and technical indicators, including NCSC-UK cybersecurity advisory "APT28 exploit routers to enable DNS hijacking operations" and CISA's Edge Device Security webpage.

Users of SOHO routers are encouraged to upgrade end-of-support devices, update to latest firmware versions, change default usernames and passwords, and disable remote management interfaces from the Internet. All users should carefully consider certificate warnings in web browsers and email clients.

Organizations that allow remote work should review relevant policies regarding how employees access sensitive data, such as using VPNs and hardened application configurations. Additionally, organizations may consider incentivizing employees to upgrade outdated personal devices involved in remote access.

Report It

If you suspect you have been targeted or compromised by a Russian GRU cyber intrusion, report the activity to your local FBI field office or file a complaint with the IC3. Be sure to provide details about your router, including device type and DHCP configurations.

Black Lotus Labs® at Lumen and Microsoft Threat Intelligence provided valuable technical contributions to this announcement. MIT Lincoln Laboratory provided assistance with testing and validation