

Russian Stockpiled Telecom-Grade Routers DML



Overview

Inside the Kremlin's Router Raids: How Russian Hackers Turned What makes this particular campaign notable isn't that Russian hackers compromised routers —.

Key Takeaways

Russian military intelligence (GRU/APT28) has exploited thousands of consumer and small-office routers worldwide to conduct espionage, DNS hijacking, and credential theft, demonstrating a sophisticated global cyber operation. Overview of the Campaign Russian military-linked threat actors, primarily APT28 (also known as Forest Blizzard, Fancy Bear, or Strontium), have been systematically targeting telecom-grade and consumer routers, including TP-Link and MikroTik models, to build covert intelligence collection infrastructure. The campaign, active since at least 2025, involved 18,000 to 40,000 compromised routers across 120 countries, with a focus on devices in homes, small offices, and remote workplaces.

These routers were exploited to intercept network traffic, harvest credentials, and redirect DNS queries to Russian-controlled servers.

Methods and Techniques

The attackers leveraged outdated firmware, default SNMP credentials, and known vulnerabilities in routers such as TP-Link WR841N, Archer C5/C7, and MikroTik WDR series. Once compromised, the routers' DNS and DHCP settings were modified, causing all connected devices to unknowingly route traffic through Russian-controlled infrastructure. This allowed the GRU to: Intercept encrypted communications and OAuth tokens for cloud services like Microsoft 365.

Harvest passwords and authentication tokens without alerting users. Use compromised routers as proxies to reach higher-value targets, including government and law enforcement networks. The operation utilized both classic attack methods and advanced tools, including large language models like LAMEHUG, to automate and scale attacks while remaining difficult to detect.

Global Response and Mitigation

In April 2026, the FBI, UK National Cyber Security Centre, Microsoft, and Lumen Technologies coordinated Operation Masquerade, a court-authorized takedown of compromised routers in the U. S., effectively neutralizing part of the infrastructure. The campaign highlighted the risks posed by stockpiled or unpatched telecom-grade routers, prompting regulatory actions such as the FCC's inclusion of foreign-made consumer routers on a Covered List to prevent importation of devices deemed a national security risk.

Implications

This campaign underscores several critical points: Telecom-grade routers are high-value targets for state-sponsored espionage due to their central role in network traffic routing. Unpatched or end-of-life devices can be weaponized at scale, affecting both personal and organizational networks.

DN

S hijacking and credential theft can bypass traditional endpoint security, making detection challenging. Global coordination among intelligence and cybersecurity agencies is essential to mitigate such threats. In summary, Russian military intelligence has demonstrated the ability to stockpile and exploit telecom-grade routers for large-scale espionage, leveraging both technical vulnerabilities and sophisticated operational planning to compromise networks worldwide.

Article Content

Inside the Kremlin's Router Raids: How Russian Hackers Turned

What makes this particular campaign notable isn't that Russian hackers compromised routers — that's been happening for years. It's the scale, the persistence, and the clear integration of

Your Router Is Spying on You — And Russia's APT28 Is Behind It

Russia's APT28 is hijacking home and office routers to steal passwords and OAuth tokens via DNS poisoning. Your home router may already be working for Russian military intelligence — and

Thousands of consumer routers hacked by Russia's military

The Russian military is once again hacking home and small office routers in widespread operations that send unwitting users to sites that harvest passwords and credential tokens for use in...

TP-Link: US operation evicts Russia from hacked SOHO routers used

The U.S. Department of Justice (DOJ) announced on Tuesday that it had dismantled a years-long cyberespionage operation by Russia's military intelligence agency, the GRU, which had

Russian Hackers Exploiting Home and Small-office

A large-scale campaign by Forest Blizzard, a Russian military-linked threat actor, targeting home and small-office routers to hijack DNS traffic and

Russian State-Linked APT28 Exploits SOHO Routers in Global DNS ...

APT28 exploits SOHO routers for global DNS hijacking and adversary-in-the-middle attacks, enabling credential theft and espionage.

APT28 Router Attacks: MikroTik TP-Link Devices Hijacked

APT28 Hijacks MikroTik and TP-Link Routers for Espionage Russia-linked APT28 group compromised insecure MikroTik and TP-Link routers since

Consumer Routers, Prohibiting Approval of New Models FACT

cations Commission updated its Covered List to include all consumer-grade routers produced in foreign .

FCC places foreign made consumer-grade routers on US ban list

The Federal Communications Commission (FCC) in the United States has taken a step to heed President Donald Trump's call to close security gaps in the United States by placing foreign

Internet Crime Complaint Center (IC3) | Russian GRU Exploiting ...

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

Internet Crime Complaint Center (IC3) | Russian GRU Exploiting ...

Russian General Staff Main Intelligence Directorate (GRU) cyber actors are exploiting vulnerable routers worldwide to intercept and steal sensitive military, government, and critical

New foreign-made routers blocked in US| Cybernews

The FCC is blocking new foreign-made consumer routers from entering the US market, citing national security risks and China-linked cyber threats targeting key infrastructure.

Russian Hackers Turned Your Home Router Into a

Russian hackers compromised thousands of home routers worldwide to steal credentials and government secrets until FBI-led operations eliminated

US operation evicts Russia from hacked SOHO routers

US operation evicts Russia from hacked SOHO routers used to breach critical infrastructure The newly disclosed cyberattack campaign is the latest

US, UK Accuse Russia of Hacking Home Routers and

Hacked devices ranged from small home routers to ISP-grade routers and firewalls, with attackers trying to hoard as many systems as possible.

Your Home Router Was a Target of Russian Military Intelligence.

Russia's APT28 unit used compromised home routers to redirect traffic and intercept credentials across 23 US states. The April 7 advisory from the FBI and NSA carried a message most

Russia Hacked Routers to Steal Microsoft Office Tokens

Hackers linked to Russia's military intelligence units are using known flaws in older Internet routers to mass harvest authentication tokens from Microsoft Office users, security experts warned ...

US Bans New Foreign-Made Routers, Citing "Unacceptable" Security

The FCC bans new foreign-made routers over national security risks, a move that could reshape the US tech supply chain and impact pricing and availability.

Contact Us

Continue your research online:

Website: <https://cgweb.co.za>

Technical inquiry: <https://cgweb.co.za/project-enquiry.html>

This document is for preliminary research. Verify specifications against current standards, product documentation and project requirements.

