Threat Intelligence Trending Topics
Russian Cyber Actors Use Compromised Routers to Facilitate Cyber Operations

Summary

- The Federal Bureau of Investigation (FBI), National Security Agency (NSA), US Cyber Command, and international partners released a joint Cybersecurity Advisory (CSA) to warn that Russia-linked threat actors are using compromised Ubiquiti EdgeRouters to evade detection in cyber operations worldwide.

Technical Details

- In February 2024, a court order allowed US authorities to neutralize the Moobot botnet, a network of hundreds of small office/home office (SOHO) routers under the control of the Russia-linked group APT28
- An FBI investigation revealed APT28 actors accessed EdgeRouters compromised by Moobot, a botnet that installs OpenSSH trojans on compromised hardware
- As early as 2022, APT28 actors had utilized compromised EdgeRouters to facilitate covert cyber operations against governments, militaries, and organizations around the world
- Targets include various industries like Aerospace & Defense, Education, Energy & Utilities, Governments, Hospitality, Manufacturing, Oil & Gas, Retail, Technology, and Transportation
- Targeted countries include US, Czech Republic, Italy, Lithuania, Jordan, Montenegro, Poland, Slovakia, Turkey, Ukraine and the UAE.
- APT28 actors have used compromised EdgeRouters to collect credentials, proxy network traffic, and host spoofed landing pages and custom post-exploitation tools.
- EdgeRouters are widely used in SmallOffice/HomeOffice (SOHO) environments and lack any effective security controls.

Campaign IOCs

- matbaiteahe[.]mooo[.]com
- lalapoc[.]kozow[.]com
- gneivaientga[.]ignorelist[.]com
- antotehlant[.]theworkpc[.]com
- onechoice[.]gleeze[.]com
- mumucnc[.]kozow[.]com

No Hits for IOCs

MITRE ATTACK

- Develop Capabilities [T1587]
- Obtain Capabilities [T1588]
- Compromise Infrastructure [T1584]
- Phishing [T1566]
- Exploitation for Client Execution [T1203]
- Event Triggered Execution [T1546]
- Adversary-in-the-Middle [T1557]
- Modify Authentication Process [T1556]
- Automated Collection [T1119]
- Automated Exfiltration [T1020]