Public Service Announcement
FEDERAL BUREAU OF INVESTIGATION

Alert Number: I-082025-PSA
August 20, 2025

Russian Government Cyber Actors Targeting Networking Devices, Critical Infrastructure

The Federal Bureau of Investigation (FBI) is warning the public, private sector, and international community of the threat posed to computer networks and critical infrastructure by cyber actors attributed to the Russian Federal Security Service's (FSB) Center 16. The FBI detected Russian FSB cyber actors exploiting Simple Network Management Protocol (SNMP) and end-of-life networking devices running an unpatched vulnerability (CVE-2018-0171) in Cisco Smart Install (SMI) to broadly target entities in the United States and globally.

In the past year, the FBI detected the actors collecting configuration files for thousands of networking devices associated with US entities across critical infrastructure sectors. On some vulnerable devices, the actors modified configuration files to enable unauthorized access to those devices. The actors used the unauthorized access to conduct reconnaissance in the victim networks, which revealed their interest in protocols and applications commonly associated with industrial control systems.

The FSB Center 16 unit conducting this activity is known to cybersecurity professionals by several names, including "Berserk Bear" and "Dragonfly," which refer to separate but related cyber activity clusters. For over a decade, this unit has compromised networking devices globally, particularly devices accepting legacy unencrypted protocols like SMI and SNMP versions 1 and 2. This unit has also deployed custom tools to certain Cisco devices, such as the malware publicly identified as "SYNful Knock" in 2015.

The FBI and law enforcement partners previously released guidance that remains relevant in a Technical Alert, "Russian State-Sponsored Cyber Actors Targeting Network Infrastructure Devices" on 20 April 2018, and a Joint Advisory, "Primary Mitigations to Reduce Cyber Threats to Operational Technology" on 6 May 2025. In addition, Cisco Talos published a blog post on 20 August 2025 with more information on their analysis of this threat actor, identified by Cisco Talos as Static Tundra.

If you suspect you have been targeted or compromised by a Russian FSB cyber intrusion, immediately report the activity to your local FBI field office or file a report on the FBI's Internet Crime Complaint Center (IC3).

- Prior to initiating a IC3 report, evaluate your router and other networking devices for any configuration changes or malware that could have been installed on the devices. Once evaluated, provide this detailed information within the IC3 report.