Updates
December 12, 2024
Salt Typhoon Cyberattacks: New Federal Cybersecurity Guidelines for Telecoms

U.S. federal agencies, including the Cybersecurity and Infrastructure Security Agency (CISA), National Security Agency (NSA), and Federal Bureau of Investigation (FBI) (in coordination with similar agencies in Australia, Canada, and New Zealand), confirmed prior reports of cyber espionage against U.S. commercial telecommunications infrastructure, among other global targets, and issued updated cybersecurity guidance for telecommunications providers and other critical infrastructure organizations in response to these threats. Senior officials in the Biden administration linked the wave of attacks to Salt Typhoon, a Chinese state-sponsored hacking group known for its sophisticated infiltration of major telecommunications systems and U.S. counterintelligence operations since at least 2020. These developments underscore the immediate need for stronger cybersecurity measures to protect communications infrastructure and networks. In addition, as discussed further below, the Federal Communications Commission (FCC) proposed a declaratory ruling and a new rulemaking proceeding to require U.S. telecoms to take steps to better protect their networks from outside cyberthreats.

Salt Typhoon

Salt Typhoon engages in cyber espionage campaigns across North America and Southeast Asia aimed at intercepting network traffic and exfiltrating sensitive data. In recent months, Salt Typhoon executed a sophisticated breach of American telecommunications systems, compromising networks of major global telecommunications providers and targeting call records, private communications, and sensitive law enforcement data. The breach included gaining access to communications of high-profile individuals, such as presidential candidates and senior government officials. While investigators are still assessing the full scope of the attack, its implications highlight the vulnerabilities within communications networks and other critical infrastructure, as well as the heightened risk of cyber espionage campaigns against both governmental and commercial targets.

Key Themes

The interagency guidance outlines actionable best practices for network engineers and defenders of communications infrastructure (as well as organizations with on-premises enterprise equipment) to strengthen visibility, secure systems, and enhance incident response capabilities. Key themes include:

1. **Strengthening visibility.**

- Monitoring network traffic rigorously, detecting anomalous activity, and logging unauthorized changes to routers, switches, and firewalls.
- Centralizing configuration management and enforcing secure, encrypted logging practices to detect security incidents in real time.
- Establishing baselines for normal network behavior and setting up alerts for deviations.

2. **Hardening systems and devices.**

- Applying timely patches and securing device configurations to minimize vulnerabilities.
- Enforcing strict access controls, including multifactor authentication, role-based permissions, and device-level segmentation.
- Disabling unused services, protocols, and virtual private networks (VPNs).

3. **Vendor-specific considerations.**

- Recognizing vulnerabilities specific to frequently targeted network equipment devices and features.
- Following network equipment manufacturer-specific hardening guidelines, including disabling unnecessary services, securing management traffic, and updating configurations with recommended encryption standards.

The FCC Responds

The FCC recently released a fact sheet covering (1) a proposed declaratory ruling that would clarify that telecommunications carriers are obligated to secure their networks against unlawful access and interception under the Communications Assistance for Law Enforcement Act and (2) a notice of proposed rulemaking that would require that telecommunications service providers establish cybersecurity risk management plans and annually certify compliance with these plans. The Senate Commerce Subcommittee also held a hearing on December 11, 2024, to evaluate the breach's implications and review industry best practices. In addition, on the same day that the CISA interagency guidance was issued, December 4, 2024, the U.S. Senate conducted a classified briefing involving key agencies, such as the FBI, FCC, and CISA. This session highlighted the scope of Salt Typhoon's espionage operations, including the theft of metadata and penetration of U.S. telecommunications networks.

Takeaways

The evolving threat landscape, highlighted by the Salt Typhoon attacks, serves as a stark reminder of the vulnerabilities within critical infrastructure and the importance of proactive cybersecurity measures. By understanding and implementing the latest federal guidance, organizations can bolster their defenses, safeguard sensitive information, and enhance resilience against sophisticated cyberthreats. As these challenges continue to grow, collaboration between industry and government remains essential to securing vital communications networks and protecting national security.

Authors

Explore more in

Technology Transactions & Privacy Law Privacy & Security Data Security Counseling and Breach Response Communications

Related insights

Update

Algorithmic Price-Fixing: US States Hit Control-Alt-Delete on Digital Collusion

Update

Stop the Stalemate: Senate Confirms NLRB Members and General Counsel