CyberShare®

www.cyber-share.org

2025 SMALL BROADBAND PROVIDER CYBER THREAT REPORT

Powered by:

4121 Wilson Blvd., Suite 1000
Arlington, VA 22203
703-351-2000
www.ntca.org

INTRODUCTION

CyberShare: The Small Broadband Provider Information Sharing and Analysis Center (ISAC), is dedicated to promoting the resiliency and continuity of operations for small network operators across the United States. By collecting and disseminating threat information, indicators and mitigation strategies from public and private sources, CyberShare facilitates critical intelligence sharing among participants to help small broadband providers recognize, analyze and respond to vulnerabilities.

This annual report compiles actionable intelligence about cyber threats targeting the telecommunications sector, with a focus on small broadband providers. These providers face an increasingly complex threat landscape, and industry resources can be expansive and difficult to apply to the unique needs of small companies. CyberShare bridges these gaps by working closely with industry partners, the federal government and other stakeholders to help members identify, prevent, mitigate and build resilience within their infrastructure. Through voluntary collaboration and intelligence sharing, CyberShare members benefit from peer-to-peer learning and best practices within a trusted network. This report leverages that collective intelligence to equip organizations with the insights needed to strengthen their cybersecurity posture and protect the communities they serve.

OUR METHODOLOGY

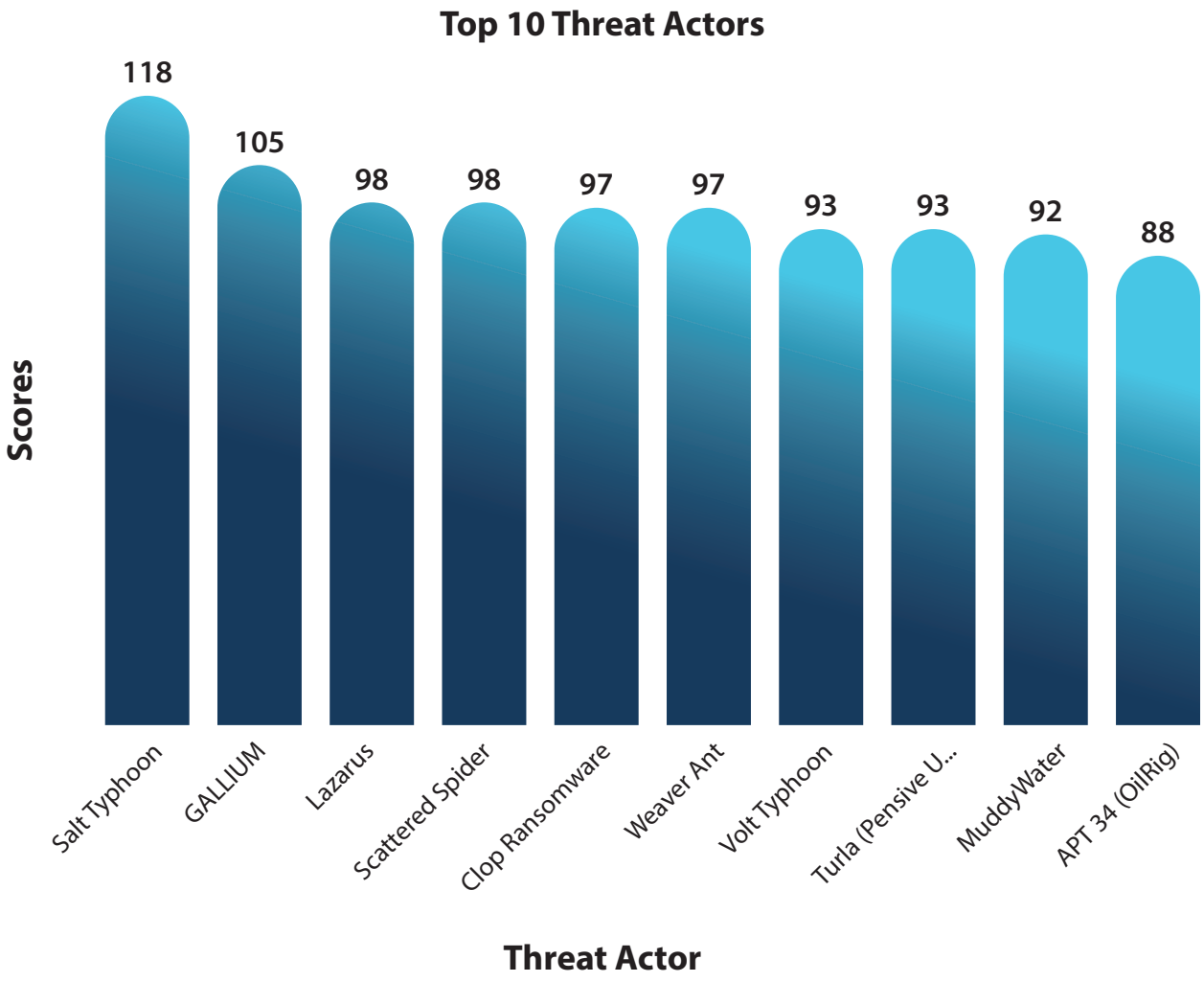
To identify and analyze actors, the CyberShare analytic team leveraged the **Predictive Adversary Scoring System (PASS),** which was developed by the analytic team in collaboration with the Information Technology-Information Sharing and Analysis Center (IT-ISAC). PASS provides a way to identify actors most relevant to specific sectors by using four key metrics:

- **Level of Activity:** How recently an adversary has been active
- **Frequency of Sector Targeting:** Number of industry specific incidents
- **Sophistication/Impact:** Complexity and effect of tactics, techniques and procedures (TTPs)
- **Motivation:** Financial, geopolitical, ideological or recognition-driven

PASS uses a scoring system of 0-128, with 128 being the highest possible score. A total of 230 adversaries were analyzed, and 34 were identified as high-risk for the industry.

TOP 10 THREAT ACTORS

The following actors represent the highest threat scores in the PASS system:



1. **Salt Typhoon (118)**
   Aliases: Earth Estries
   Summary: Chinese state-sponsored group exploiting Cisco vulnerabilities (e.g., CVE-2023-20198) and using Living off the Land (LOTL) binaries.
   Mitigation: Patch Cisco devices, monitor LOTL activity and enforce multi-factor authentication (MFA).

2. **GALLIUM (105)**
   Summary: Chinese espionage advanced persistent threat (APT) using custom malware (e.g., PingPull) across Asia, Africa and Europe.
   Mitigation: Deploy endpoint detection and response (EDR), segment networks and monitor custom malware.

3. **Lazarus (98)**
   Aliases: HIDDEN COBRA, ZINC, Diamond Sleet
   Summary: North Korean group targeting telecommunications companies for financial theft and espionage.
   Mitigation: Patch zero-days, monitor phishing and apply behavioral analytics.

4. **Scattered Spider (98)**
   Aliases: Roasted 0ktapus, Octo Tempest
   Summary: Financially motivated group using SIM swapping and social engineering.
   Mitigation: Enforce MFA, monitor remote monitoring and management (RMM) tools.

5. **Clop Ransomware (97)**
   Aliases: FIN11, TA505
   Summary: Russian-speaking ransomware as a service (RaaS) group exploiting MOVEit for double extortion.
   Mitigation: Patch exposed systems, backup regularly, monitor egress traffic.

6. **Weaver Ant (97)**
   Summary: Chinese espionage group with encrypted backdoors and long-term persistence.
   Mitigation: Monitor encrypted channels, apply anomaly detection, vet software.

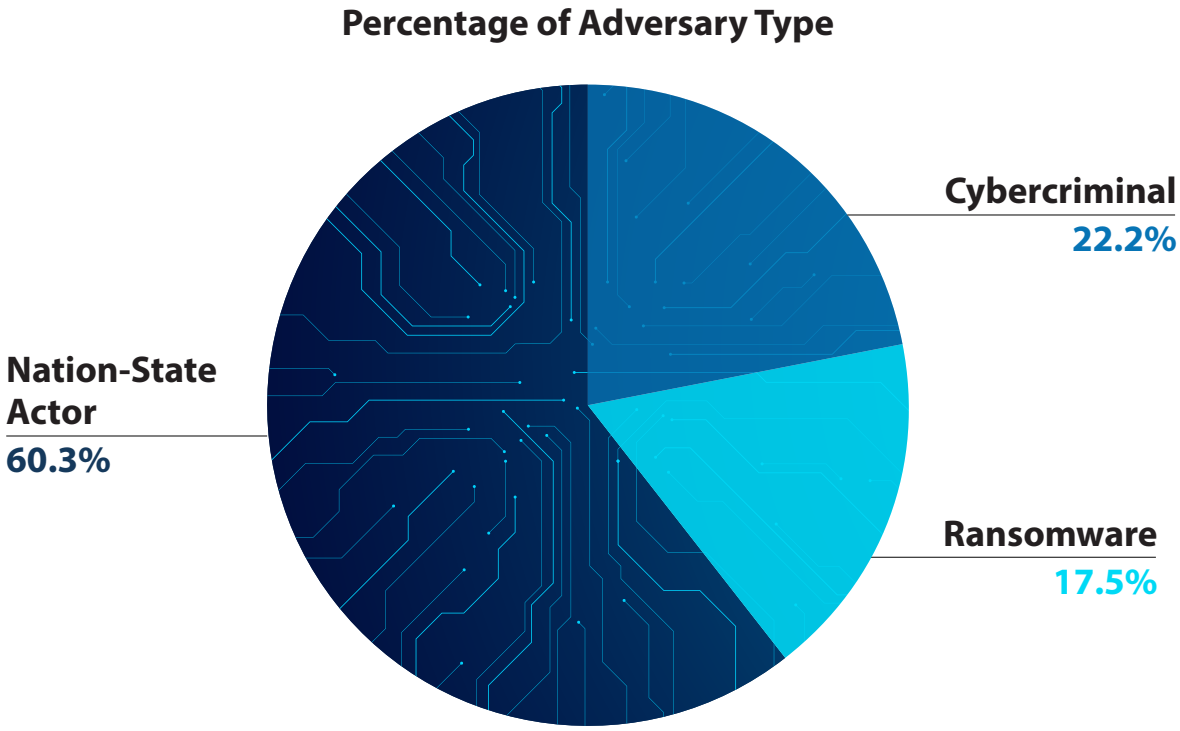
7. **Volt Typhoon (93)**
   Summary: Chinese APT using stolen credentials and admin tools for U.S. infrastructure infiltration.
   Mitigation: Implement zero-trust security, monitor administrative activity and harden credentials.

8. **Turla (93)**
   Aliases: Pervasive Union
   Summary: A Russian FSB-linked group is using malware such as Snake and satellite command and control (C2).
   Mitigation: Monitor C2 traffic, deploy EDR, update malware defenses.

9. **MuddyWater (92)**
   Summary: Iranian MOIS-linked group using spear phishing and PowerShell tools.
   Mitigation: Monitor PowerShell, enhance domain name system (DNS) visibility and train staff on phishing.

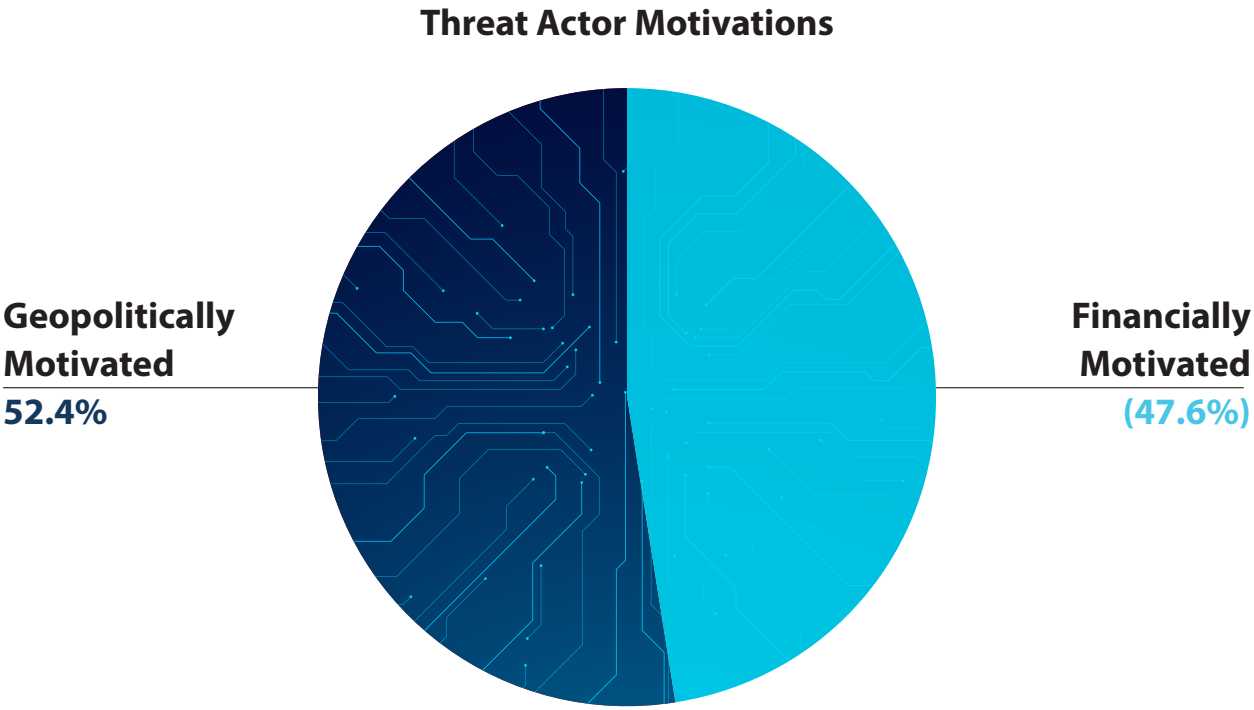
10. **APT34 / OilRig (88)**
    Aliases: Helix Kitten, Hazel Sandstorm
    Summary: Iranian group using malware (e.g., Helminth) to target Middle Eastern telecommunication companies.
    Mitigation: Monitor web shells, DNS tunneling and credential theft.

SUMMARY OF ADVERSARY TYPES



- **Nation-State Actors (60.3%)**
  - Nation-state actors are typically sponsored or directed by governments and target the telecommunications sector for strategic objectives. These include long-term espionage campaigns, intellectual property theft, disruption of critical infrastructure and surveillance.
  - (Examples: Salt Typhoon, Volt Typhoon)
- **Cybercriminals (22.2%)**
  - Cybercriminal groups are primarily motivated by financial gain. They engage in access brokering, data theft and resale of sensitive information, often targeting telecommunications firms for monetizable assets or customer data.
  - (Example: Scattered Spider)
- **Ransomware Operators (17.5%)**
  - These groups use ransomware to encrypt systems and demand payment, often employing double extortion by threatening public leaks. They may exploit third-party software or supply chains to access telecommunications networks.
  - (Examples: Clop, LockBit 3.0)

SUMMARY OF THREAT ACTOR MOTIVATION



Threat actor motivation is **roughly split** between:

- **Geopolitical Drivers (52.4%)**

  Nation-state actors target telecommunications infrastructure to disrupt operations, steal sensitive data and gain strategic or geopolitical advantage.

- **Financial Drivers (47.6%)**

  Cybercriminal and ransomware groups pursue financial gain through extortion, leveraging tactics such as ransomware deployment and data exfiltration. Some nation-state actors also are motivated by financial gain.

SUMMARY OF TACTICS, TECHNIQUES, AND PROCEDURES (TTPS), TOP 5:

Percentage of Threat Actor TTPs

- **Targeted Spear Phishing (61%)**
  - Spear phishing involves sending highly targeted, deceptive emails to trick recipients into revealing credentials or downloading malware.
  - *Mitigation*: User training, anti-phishing tools, domain verification
- **Living-Off-the-Land (LOTL) Techniques (60%)**
  - LOTL techniques utilize legitimate system tools and processes (e.g., PowerShell, Windows Management Instrumentation (WMI)) to conduct malicious activity while evading detection.
  - *Mitigation*: Application allow listing, living off the land binaries (LOLBin) monitoring, segmentation.

- **Zero-Day Exploits (59%)**
    - Zero-day exploits exploit previously unknown vulnerabilities in software or hardware before patches are available.
    - *Mitigation*: Join ISACs, monitor open source intelligence (OSINT) and apply anomaly detection.
- **Disruptive Tactics (57%)**
    - These tactics include ransomware attacks, DDoS campaigns and other techniques designed to interrupt telecommunications operations and force ransom payments.
    - *Mitigation*: Backups, redundancy, business continuity planning
- **Supply Chain Compromise (55%)**
    - This method targets vulnerabilities in third-party software, vendors or services to gain indirect access to telecommunications networks.
    - *Mitigation*: Vet third parties, enforce least privilege, review software vendors

GENERAL MITIGATION GUIDELINES

Understanding threat actors, their motivations and their TTPs can help companies take action to defend against specific threats and actors. However, defending against cyber threats requires companies to take a range of defensive measures. Sound security practices can include:

- **Implement Multi-Factor Authentication (MFA)**

  Require multiple forms of identity verification to reduce the risk of unauthorized access.
- **Adopt Zero Trust Architecture**

  Assume no user or system is trusted by default; enforce strict access controls and continuous verification.
- **Regularly Patch Vulnerabilities**

  Apply security updates promptly to protect systems from known exploits.
- **Conduct Phishing Awareness Training**

  Educate staff on identifying and avoiding phishing attempts, with regular simulated testing.
- **Monitor Admin Tools and Encrypted Channels**

  Track the use of privileged tools and encrypted traffic to detect abuse or malicious activity.
- **Ensure Robust Business Continuity Plans**

  Prepare for operational disruptions with tested backup, recovery and continuity strategies.

STRENGTHENING YOUR ORGANIZATION THROUGH CYBERSHARE

The threat landscape facing small broadband providers continues to evolve at an accelerating pace. Nation-state actors, cybercriminals and ransomware operators are becoming more sophisticated, more persistent and more focused on critical communications infrastructure.

This report represents just one element of CyberShare's comprehensive intelligence-sharing mission. Through CyberShare, organizations gain access to a trusted network of industry and government experts who are actively monitoring emerging threats and developing real-time mitigation strategies. By participating in a collaborative defense model, companies benefit from the collective experience of more than 150 small broadband providers facing the same challenges.

The value of participating in CyberShare extends beyond technical intelligence. Members build relationships with peers and deepen their understanding of evolving threats, demonstrating a prioritization of the security of your company, customers and community.

Become part of a community committed to the continuous improvement of cybersecurity practices across the rural broadband sector. Learn more at www.cyber-share.org

JOIN 150+ SMALL BROADBAND PROVIDER MEMBER COMPANIES AND JOIN CYBERSHARE. AS A MEMBER, YOU'LL HAVE ACCESS TO:

- **24 peer-to-peer threat sharing calls a year with government and industry leaders**
- **Daily intelligence reports**
- **Access to analysts and weekly technical reports specifically tailored to small broadband providers**

CyberShare®