

CyberShare®

www.cyber-share.org

2026 SMALL BROADBAND PROVIDER CYBER THREAT REPORT

Powered by: NTCA THE RURAL BROADBAND ASSOCIATION®

© 2026 NTCA–The Rural Broadband Association
4121 Wilson Blvd., Suite 1000
Arlington, VA 22203
703-351-2000
www.ntca.org

TABLE OF CONTENTS

- INTRODUCTION 3
- PASS EXPLAINED 4
- TOP 10 THREAT ACTORS 5
- SUMMARY OF ADVERSARY TYPES 11
- SUMMARY OF THREAT ACTOR MOTIVATION 12
- SUMMARY OF TTPS USED BY ADVERSARIES 13
- TOP MITRE ATT&CK TECHNIQUES 15
- TOP 10 CVES ABUSED 17
- FULL FINDINGS 18

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.

To support these efforts, CyberShare leveraged the Predictive Adversary Scoring System (PASS), which helps analysts identify and prioritize known cyber adversaries active in the sector. This enables CyberShare members to prioritize defensive practices against relevant threat actors and scores adversaries on various parameters, including their ability, intent and past behavior. By understanding the tactics, techniques and procedures (TTPs) of the threat actors active in the industry, companies can make informed risk management decisions and allocate their limited resources to maximum effect.

The telecommunications sector faces a dynamic and evolving cyberthreat landscape. While much attention is focused on high-profile advanced nation-state actors, the sector combats a range of actors, including financially motivated cybercriminal groups. While the report focuses on the telecommunications industry, it also highlights the interconnected risks that span multiple industries, underscoring that no sector is immune and indeed most sectors are interdependent.

PASS EXPLAINED

PASS is a comprehensive scoring system that helps organizations assess their risk exposure and allocate resources effectively. It evaluates adversarial risk through four key metrics:

- **Level of Activity:** How recently the adversary has been active.
- **Frequency of Sector Targeting:** The number of times the adversary has targeted the telecommunications sector.
- **Sophistication/Impact:** The complexity of the adversary's tactics, techniques and procedures (TTPs) and their impact.
- **Motivation:** The driving force behind the adversary – financial, geopolitical, ideological or recognitional.

This report researched threat actors with a history of targeting the telecommunications industry. Of the 330 actors monitored, PASS identified 35 distinct adversaries with recorded attacks that directly impacted telecommunications organizations.

The PASS system employs a comprehensive set of metrics to assign adversaries a score ranging from 0 to a maximum of 100, representing the highest level of threat achieved when a threat actor satisfies all of the system's predefined criteria. The higher scores indicate a greater level of risk to organizations within the sector. Adversaries with elevated scores represent significant threats due to their frequent targeting of the sector and their demonstrated sophistication and impact in past operations.

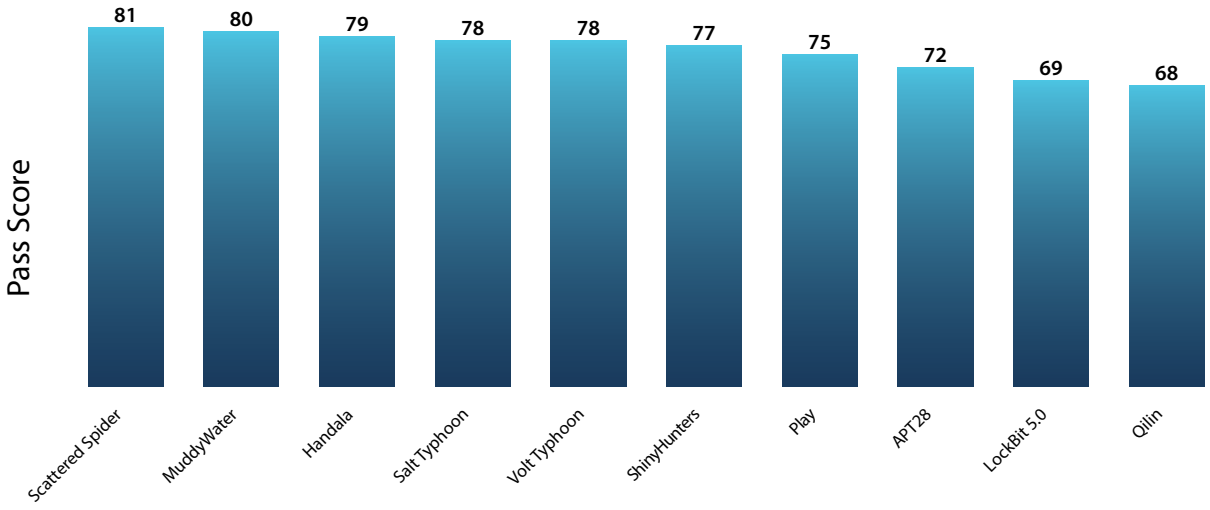
This report was created with the help of Conrad Inc.

Conrad, Inc.
CYBERSECURITY CONSULTING

TOP 10 THREAT ACTORS

The following actors have been highlighted for their outsized impact on the sector, scoring 68 and above on the PASS scale. The TTPs referenced below are MITRE ATT&CK® techniques.

Top 10 Threat Actors



SCATTERED SPIDER

Type:
Cybercriminal

Motivation:
Financial

Top TTPs:
T1078 - Valid Accounts (Initial Access)
T1621 - MFA Request Generation (Credential Access)
T1566.002 - Spear Phishing Link (Initial Access)
T1136 - Create Account (Persistence)
T1486 - Data Encrypted for Impact (Impact)

Scattered Spider (also tracked as UNC3944, Octo Tempest, or Muddled Libra) is among the most critical threat actors for telecommunications organizations to monitor. The group emerged through SIM-swapping campaigns, socially engineering mobile carriers into transferring active SIM cards to actor-controlled devices, then using those devices to reset passwords and commit financial theft.

It has remained highly active since, running social engineering campaigns that are relatively simple but highly effective. Its operatives are largely young and native English-speaking; they understand Western corporate structures, use internal jargon flawlessly, and pivot quickly between extortion, data theft and ransomware deployment.

Unlike state-sponsored groups that rely on zero-day exploits, Scattered Spider exploits employees. Customer service reps and IT help desks are favorite targets because they are conditioned to be helpful and to resolve lockouts quickly. The group maps target organizations using LinkedIn, public records and dark web credential dumps, looking specifically for help desk staff, IT administrators and third-party vendors. Operators then call the help desk posing as an employee in an urgent account crisis or deploy reverse-proxy phishing frameworks on look-alike domains to capture session cookies and credentials in real time.

They also use MFA bombing, flooding an employee's phone with login approval prompts until one is approved, deliberately or by accident. Once inside, they do not immediately execute malware. Instead, they blend in using legitimate built-in tools and routinely compromise Slack and Microsoft Teams to watch how the security team is responding to them.

MUDDYWATER

Type:



Nation-state

Motivation:



Geopolitical

Top TTPs:
T1059.001 - PowerShell (Execution)
T1219 - Remote Access Software (Command and Control)
T1566.001 - Spear Phishing Attachment (Initial Access)
T1190 - Exploit Public-Facing Application (Initial Access)
T1102 - Web Service (Command and Control)

MuddyWater is a key cyber component of Iran's Ministry of Intelligence and Security (MOIS), and telecommunications providers have long been a high-priority target. The group collects strategic intelligence such as subscriber data, call detail records (CDRs) and network topologies to feed broader geopolitical monitoring. Because telecommunications providers and MSPs hold trusted connections into their customers' networks, MuddyWater uses a single compromise to pivot into government agencies, defense contractors and financial institutions. It maps victim networks and shares or sells that persistent access to other Iranian state-aligned actors. MuddyWater usually keeps a low profile for continuous collection but has deployed ransomware both for destructive effect and to mask data exfiltration.

For initial access, it compromises supply chain partners' email and Microsoft Teams accounts, then uses those trusted channels to send malicious attachments to the real target. Smaller vendors are a route to their larger partners, and companies that host data for multiple clients are attractive because one compromise yields many victims. Historically MuddyWater relied on PowerShell scripts, Python downloaders and RMM tools like Atera, ScreenConnect and SimpleHelp. As EDR has adapted to those techniques, the group has shifted to custom malware compiled in Rust and Go to evade traditional antivirus signatures.

HANDALA

Type:



Hacktivist

Motivation:



Ideological

Top TTPs:
T1485 - Data Destruction (Impact)
T1566.001 - Spear Phishing Attachment (Initial Access)
T1059.001 - PowerShell (Execution)
T1021.001 - Remote Desktop Protocol (Lateral Movement)
T1003.001 - LSASS Memory (Credential Access)

Though it presents itself as a pro-Palestinian hacktivist collective, global intelligence agencies and cybersecurity firms widely assess Handala to be a state-directed front for Iran's MOIS. Telecommunications networks are high-value targets for Handala because they sit at the intersection of critical infrastructure, sensitive user data and mass communication channels. In past campaigns, they have compromised telecommunications infrastructure or used stolen databases to send threatening mass SMS broadcasts to citizens, turning compromised networks into psychological warfare tools.

Handala's end goal is disruption rather than profit. It deploys wiper malware to destroy system data and corrupt master boot records, using ransomware as a distraction. Before wiping, it exfiltrates large volumes of customer and corporate data, later releasing it on leak sites and Telegram to maximize reputational damage.

For initial access, Handala targets VPN gateways with compromised credentials, masking its origin through commercial VPN nodes. It also exploits known vulnerabilities in internet-facing servers such as Microsoft SharePoint to drop ASPX web shells for persistence and has been observed abusing administrative tools like Microsoft Intune and group policy objects to push payloads downstream.

Once inside, the group enumerates Active Directory and moves laterally via RDP before running multiple wiper scripts simultaneously, targeting both Windows and Linux systems.

SALT TYPHOON

Type:

Nation-state

Motivation:

Geopolitical

Top TTPs:
T1190 - Exploit Public-Facing Application (Initial Access)
T1078 - Valid Accounts (Initial Access)
T1098 - Account Manipulation (Persistence)
T1572 - Protocol Tunneling (Command and Control)
T1574.002 - DLL Side-Loading (Persistence)

Salt Typhoon is a sophisticated Chinese threat actor also tracked as GhostEmperor or UNC2814. It targets the signaling and routing systems at the internet's backbone, sweeping up call detail records (CDRs) and using that metadata to build comprehensive social maps of its targets. By embedding within major ISPs, the group puts anyone relying on those networks such as government agencies, businesses and millions of citizens within reach of interception.

Most notably, Salt Typhoon has demonstrated the ability to compromise lawful interception systems, the channels legally mandated for court-ordered wiretaps. That access reveals who law enforcement is investigating while letting the group wiretap diplomatic, military and corporate targets of its own choosing.

The group does not simply compromise endpoints. It embeds itself in core routing and switching infrastructure, deep inside carrier systems where antivirus and EDR software cannot run. Current activity focuses on intelligence gathering, but control of core routing protocols also gives it a latent "kill switch" to disrupt communications during a geopolitical crisis.

VOLT TYPHOON

Type:

Nation-state

Motivation:

Geopolitical

Top TTPs:
T1190 - Exploit Public-Facing Application (Initial Access)
T1078 - Valid Accounts (Initial Access)
T1003.003 - NTDS (Credential Access)
T1090.002 - External Proxy (Command and Control)
T1505.003 - Web Shell (Persistence)

Unlike most China-sponsored actors, Volt Typhoon, another Chinese adversary, is focused on sabotage and operational disruption. U.S. intelligence and cybersecurity agencies (CISA, NSA, FBI) assess with high confidence that Volt Typhoon's objective is to "pre-position" themselves inside critical infrastructure to disrupt communications and operations in the event of a geopolitical crisis.

By compromising an ISP, attackers gain access to the routing, transit and data streams of thousands of downstream critical infrastructure organizations, such as power, water and transportation.

The group seeks persistent access to information technology (IT) networks before pivoting into operational technology (OT) networks, the systems that control physical valves, switches and power grids. For telecommunications specifically, the group focuses on edge routing equipment and core internet transit infrastructure, effectively letting them control or shut down digital communication.

SHINYHUNTERS

Type:



Cybercriminal

Motivation:



Financial

Top TTPs:
T1078 - Valid Accounts (Initial Access)
T1566.004 - Spear Phishing Voice (Initial Access)
T1528 - Steal Application Access Token (Credential Access)
T1213 - Data from Information Repositories (Collection)
T1567 - Exfiltration Over Web Service (Exfiltration)

ShinyHunters (tracked as UNC6040 and closely associated with the Scattered Spider and "The Com" cybercriminal ecosystems) operates without nation-state backing but has established a highly effective playbook against telecommunications and third-party service providers. Rather than attacking network vulnerabilities directly, it exploits SaaS ecosystems such as Salesforce and Google Cloud, along with vendor integrations, to gain initial access.

Telecommunications companies hold customer names, Social Security numbers, CDRs and location data; this material commands a premium on dark web forums and gives the group substantial leverage during extortion. Because it operates with legitimate credentials, API integrations and OAuth tokens, traditional intrusion detection systems often miss its footprint. An ISP's incident response team may spend the first 48 hours hunting for malware or encryption artifacts that do not exist.

The group's social engineering is sophisticated: operators use conversational AI voice tools such as Vapi and Bland AI to impersonate IT support, then trick employees into installing modified utility apps like custom Salesforce Data Loaders or flood them with MFA prompts until one is approved.

PLAY

Type:



Ransomware

Motivation:



Financial

Top TTPs:
T1486 - Data Encrypted for Impact (Impact)
T1190 - Exploit Public-Facing Application (Initial Access)
T1078 - Valid Accounts (Initial Access)
T1059.001 - PowerShell (Execution)
T1003 - OS Credential Dumping (Credential Access)

Since its emergence in mid-2022, this group has grown into one of the most prolific and technically aggressive ransomware threats. Federal agencies (including the FBI and CISA) have tracked over 900 victim organizations worldwide. Telecommunications carriers and ISPs make highly attractive targets for Play due to the massive volume of customer data they hold, their role as critical infrastructure and the potential to use them as a stepping stone to compromise downstream business clients. According to a TrendMicro report, between June 2022 and May 2023, telecommunications was the most targeted sector by volume by the Play ransomware group.

Unlike many ransomware-as-a-service (RaaS) operations that rely solely on public malware, Play developers actively build custom .NET tools like Grixba (used for network/software enumeration) and custom Volume Shadow Copy copying tools to bypass native Windows backup protections.

APT28

Type:



Nation-state

Motivation:



Geopolitical

Top TTPs:
T1566.001 - Spearphishing Attachment (Initial Access)
T1110.003 - Password Spraying (Initial Access)
T1003 - OS Credential Dumping (Credential Access)
T1190 - Exploit Public-Facing Application (Initial Access)
T1059.001 / .003 - Command & Scripting Interpreters (Execution)

APT28 is a prolific Russian nation-state actor with a long history of campaigns. While they have historically targeted government and defense sectors, their operations have heavily shifted toward exploiting networking infrastructure and telecommunications systems.

Rather than just attacking endpoint devices like PCs, APT28 frequently focuses on routers, switches and network gateways as their primary targets. By compromising edge routers, APT28 can bypass traditional perimeter security like firewalls and position themselves within trusted network boundaries. They routinely hijack consumer and enterprise-grade routers (such as Ubiquiti EdgeRouters, Cisco, TP-Link and MikroTik) to build vast, decentralized botnets. They use this hijacked infrastructure to host phishing landing pages, proxy state-sponsored traffic and execute further brute-force attacks while masking their true Russian origin.

By taking control of ISP-grade routing equipment, they can execute adversary-in-the-middle (AitM) attacks and perform DNS hijacking. This allows them to silently redirect web traffic, capture unencrypted credentials, and route user traffic through malicious proxy networks.

LOCKBIT 5.0

Type:



Ransomware

Motivation:



Financial

Top TTPs:
T1562.001 - Impair Defenses: Disable or Modify Tools (Defense Evasion)
T1486 - Data Encrypted for Impact (Impact)
T1490 - Inhibit System Recovery (Impact)
T1055 - Process Injection (Execution)
T1070.001 - Indicator Removal: Clear Windows Event Logs (Defense Evasion)

LockBit 5.0 targets the technical foundation of modern ISPs. Telecommunications providers run heavily virtualized environments, using hypervisors to orchestrate everything from internal databases to network functions virtualization (NFV). LockBit 5.0 ships custom-built Linux and ESXi encryptors aimed at virtual machine datastores, so a single compromised hypervisor host can paralyze dozens of virtualized services at once.

LockBit's RaaS model is sector-agnostic, meaning affiliates hit any reachable organization but telecommunications firms are consistent with known victimology given their large network infrastructure, billing systems and customer databases. The 5.0 ecosystem's cross-platform tooling raises that baseline threat.

QILIN

Type:



Ransomware

Motivation:



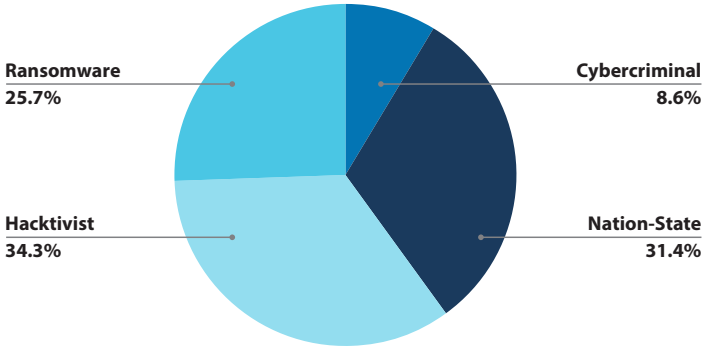
Financial

Top TTPs:
T1486 - Data Encrypted for Impact (Impact)
T1490 - Inhibit System Recovery (Impact)
T1190 - Exploit Public-Facing Application (Initial Access)
T1059.001 - PowerShell (Execution)
T1562.001 - Impair Defenses: Disable or Modify Tools (Defense Evasion)

Qilin emerged in 2022 and has since become one of the most aggressive and structurally sophisticated RaaS operations in the landscape. It has led all ransomware actors by volume since 2025, having absorbed affiliates displaced by the takedowns and collapses of LockBit and ALPHV/BlackCat, a migration driven by Qilin's revenue split, which gives affiliates 80 to 85 percent of the ransom. The group moved its core codebase from Go to Rust, producing malware that is efficient, evasive against traditional antivirus detection, able to target Windows and Linux/VMware ESXi environments equally well. Qilin also invests in psychological pressure. Its ecosystem includes DDoS capabilities to flood victim portals, in-house writers who draft public shaming articles, and a "Call Lawyer" feature in the negotiation portal that simulates legal escalation.

SUMMARY OF ADVERSARY TYPES

Percentage of Adversary Type



Hacktivists

Recent geopolitical conflicts have contributed to increased hacktivist targeting of U.S. critical infrastructure. Unlike nation-state actors, which generally prioritize stealth and persistence, hacktivists often seek visible disruption.

Nation-State Actors

Nation-state actors were the second-largest category of telecommunications adversaries. Compromising an internet service provider (ISP) can provide access to communications, internet traffic and call detail records (CDRs), allowing adversaries to conduct surveillance and map social or professional networks.

Ransomware

Of the nearly 4,200 ransomware attacks tracked through Q2 2026, 127 targeted the communications sector, representing approximately 3% of total activity. While the sector accounts for a relatively small share of ransomware activity, successful attacks can have broad consequences because outages may affect thousands of customers and critical services simultaneously.

Ransomware can disrupt essential ISP systems used to provision, manage and troubleshoot services, potentially affecting businesses, healthcare providers, public safety agencies and local governments. Ransomware actors may also steal sensitive customer and network data for extortion or use in future attacks.

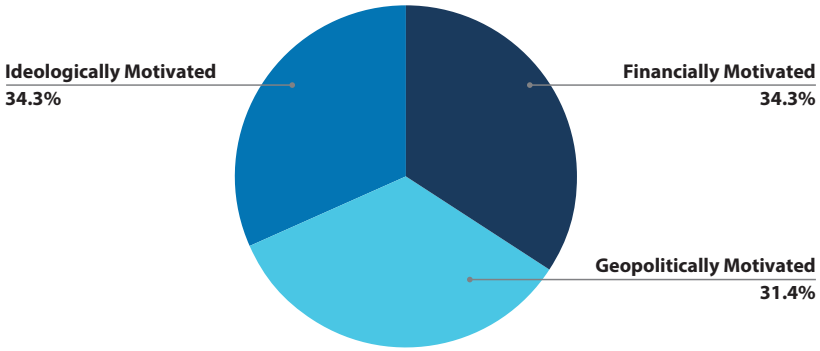
Cybercriminals

Cybercriminal groups represented the smallest category in the 2026 report, partly because more financially motivated groups now incorporate ransomware and are categorized accordingly.

Other cybercriminal activity includes initial access brokers (IABs), which compromise organizations and sell access to other threat actors, business email compromise and domain spoofing used to facilitate fraud, and DDoS-for-hire services that enable disruptive attacks using networks of compromised devices.

SUMMARY OF THREAT ACTOR MOTIVATION

Threat Actor Motivations

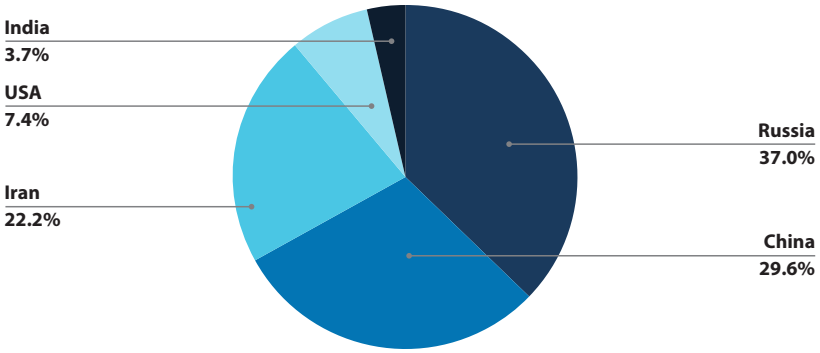


Geopolitically motivated attacks generally seek to disrupt operations, obtain sensitive information or weaken strategic rivals, often in support of broader state interests.

Financially motivated actors primarily seek monetary gain through tactics such as data theft, system encryption and extortion.

Ideologically motivated actors, including hacktivist and cybercriminal groups, typically conduct attacks in support of a political, social or religious cause.

Country Distribution



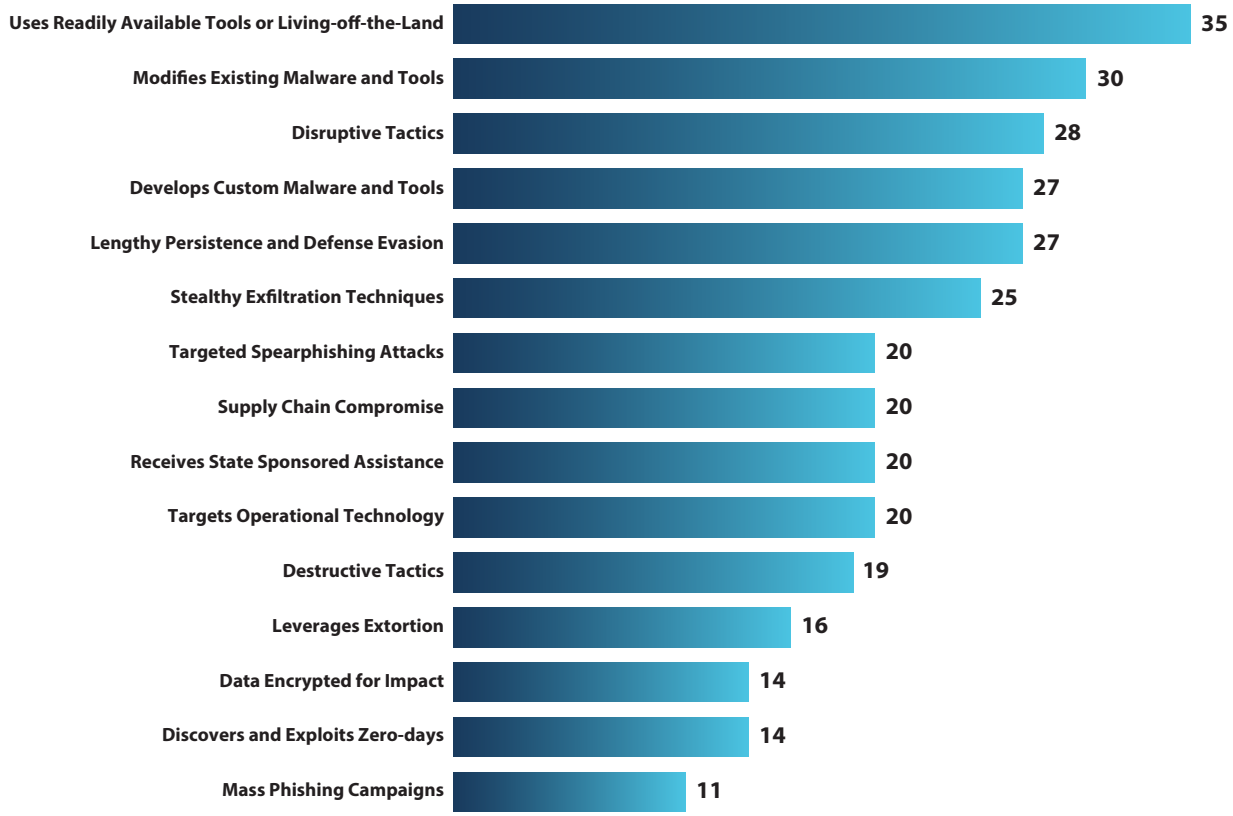
Russia: Russia accounted for the largest share of tracked threat actors, including nation-state, ransomware and cybercriminal groups. Russia has historically provided a permissive environment for cybercriminal activity originating within its borders.

China: Chinese actors have historically targeted telecommunications networks for long-term access and espionage. More recent activity has raised concerns about pre-positioning within critical infrastructure for potential disruption during a future conflict. Increased hacktivist activity has also expanded the number of China-based actors tracked.

Iran: Iranian actors have increasingly favored disruptive and destructive operations. In early 2026, CyberShare joined other ISACs in issuing an advisory detailing the Iranian cyberthreat and associated threat actors.

SUMMARY OF TACTICS, TECHNIQUES AND PROCEDURES (TTPS) USED BY ADVERSARIES

Most Common Sophistication Techniques



Uses Readily Available Tools or Living-off-the-Land (LOTL)

Every adversary assessed showed evidence of using living-off-the-land (LOTL) techniques. Rather than deploying custom malware, LOTL attacks use legitimate, pre-installed administrative tools, system binaries and scripting languages to conduct malicious activity. Because these tools are trusted and commonly used, attackers can more easily blend into normal network activity and evade detection.

Modifies Existing Malware and Tools

Roughly 86% of adversaries observed modified existing malware and tools instead of developing their own custom strains. Developing software is hard, and developing highly resilient, stealthy malware is even harder.

Disruptive Tactics

Eighty percent of the adversaries carried out disruptive attacks. Common disruptive attacks include DDoS attacks, which are highly impactful but often short-lived. These attacks overwhelm public-facing infrastructure, often making email, websites and other services unavailable.

Develops Custom Malware and Tools

While modifying existing malware was more common, 77% of adversaries developed proprietary custom malware for use in campaigns. Buying commercial off-the-shelf malware or modifying existing open-source tools is cheaper and faster, but highly sophisticated and well-resourced adversaries often choose to build custom malware from scratch.

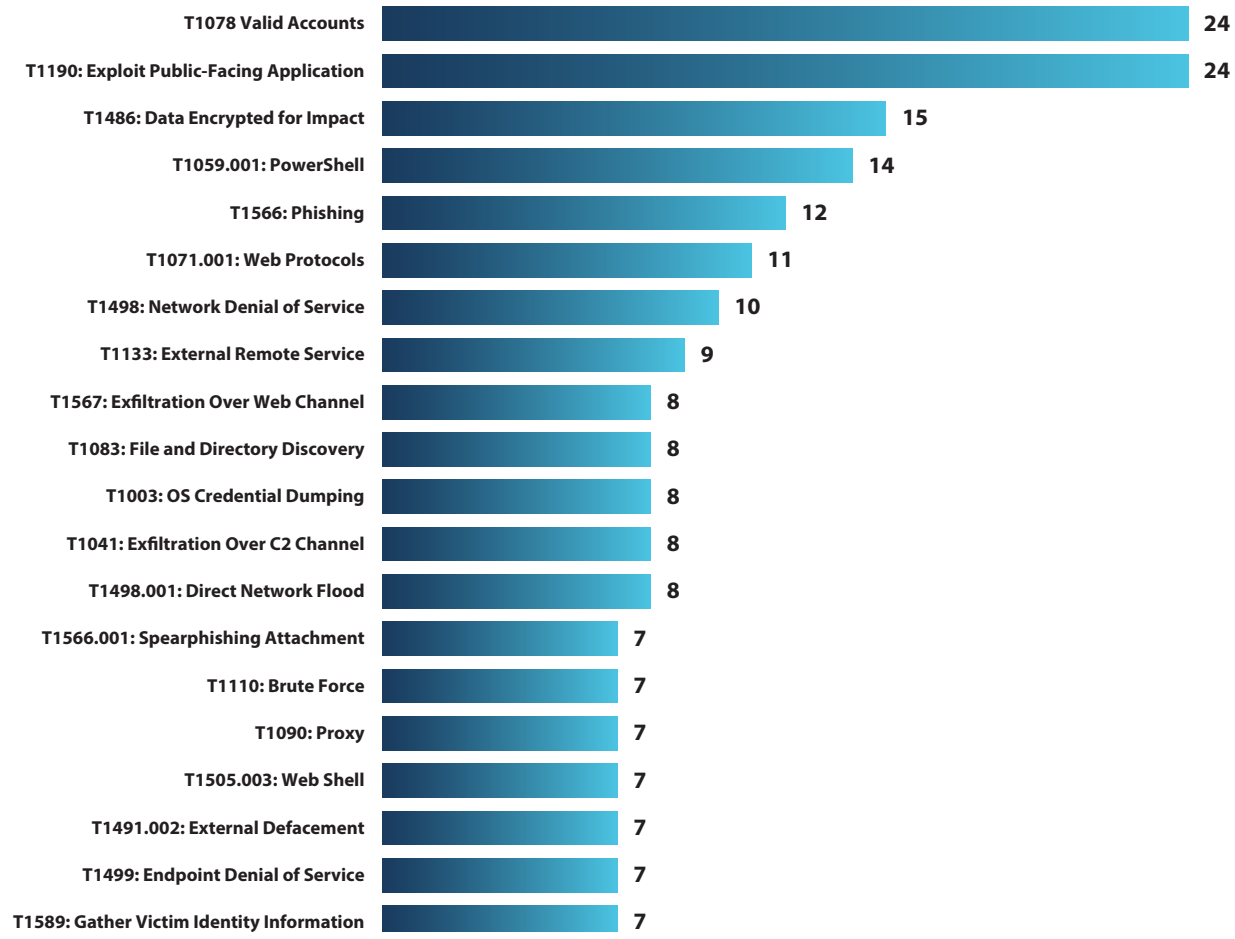
Custom malware allows adversaries to exploit brand-new vulnerabilities (zero-days) with proprietary code that has never been seen in the wild. Security systems have no signatures to flag, allowing the attack to slip by unnoticed.

Lengthy Persistence and Defense Evasion

Seventy-seven percent of adversaries used tactics designed to maintain persistent access and evade detection. Nation-state actors may remain undetected while conducting espionage, while initial access brokers maintain access until it can be sold to other threat actors.

TOP MITRE ATT&CK TECHNIQUES

Most Common MITRE ATT&CK Techniques Across All Profiles



T1078: Valid Accounts

Sixty-nine percent of adversaries used valid accounts to gain or maintain access to target environments. This technique uses legitimate credentials, API keys or access tokens obtained through methods such as phishing, credential theft or purchase from initial access brokers.

MITRE identifies four valid account sub-techniques:

- T1078.001: Default Accounts — Vendor-provided or default credentials for hardware and software.
- T1078.002: Domain Accounts — Accounts centrally managed within an enterprise network, such as through Active Directory.
- T1078.003: Local Accounts — Accounts providing access to a specific system rather than the broader domain.
- T1078.004: Cloud Accounts — Cloud or SaaS identities managed through platforms such as Microsoft Entra ID, AWS IAM or Okta.

T1190: Exploit Public-Facing Application

Sixty-nine percent of adversaries exploited vulnerabilities in public-facing applications. Internet-facing systems are routinely scanned for known vulnerabilities, allowing threat actors to quickly identify and exploit unpatched systems.

This technique is a common initial access vector for ransomware and other threat actors, particularly following the disclosure of new vulnerabilities. AI-assisted tools may further accelerate vulnerability discovery and exploitation. Timely patching and limiting unnecessary internet exposure remain critical defenses.

T1486: Data Encrypted for Impact

Forty-three percent of adversaries used data encryption to disrupt victim operations. While most closely associated with ransomware, encryption is also used by nation-state and hacktivist actors in disruptive or destructive campaigns. Adversaries may use custom ransomware or legitimate tools, such as Microsoft BitLocker, to encrypt data.

Organizations should maintain tested backups of critical data, including offline backups isolated from production environments.

T1059.001: PowerShell

Forty percent of adversaries used PowerShell, a built-in Windows command-line and scripting tool commonly leveraged in living-off-the-land (LOTL) attacks. Its legitimate administrative capabilities allow adversaries to execute commands, access system resources and conduct malicious activity while reducing reliance on detectable malware.

Where operationally feasible, PowerShell access should be restricted and its activity monitored for suspicious commands and behavior.

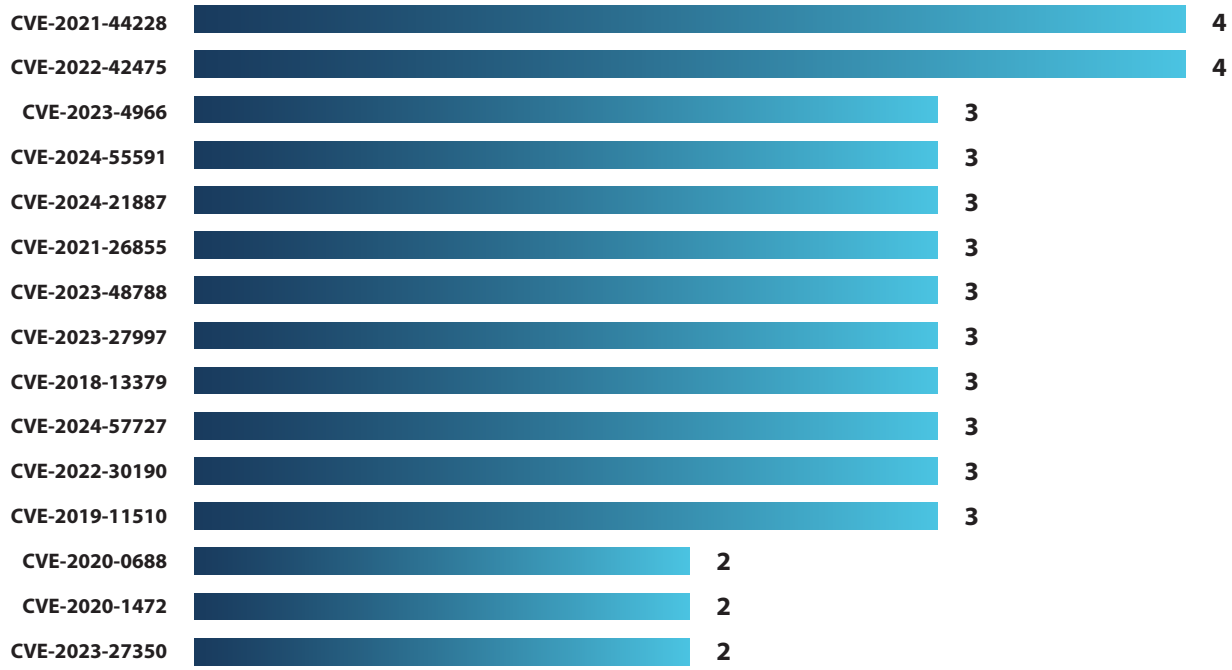
T1566: Phishing

Thirty-four percent of adversaries used phishing techniques. The relatively low percentage may reflect the difficulty of attributing phishing campaigns to specific threat actors rather than limited use of the technique. Phishing remains an effective method for obtaining legitimate credentials and gaining initial access across a wide range of adversaries.

Regular security awareness training and effective reporting procedures can help organizations identify and contain phishing attempts before they result in broader compromise.

TOP 10 COMMON VULNERABILITIES AND EXPOSURES (CVES) ABUSED

Most Common CVEs Across All Profiles



Several vulnerabilities were repeatedly associated with the adversaries assessed. All appear in CISA's Known Exploited Vulnerabilities (KEV) Catalog, indicating evidence of active exploitation. Organizations should prioritize remediation of KEV-listed vulnerabilities, particularly those affecting internet-facing systems.

Target Category	Products	Vulnerabilities
Edge VPN, Firewall & Gateway	Fortinet, Ivanti/Pulse, Citrix	CVE-2018-13379; CVE-2019-11510; CVE-2022-42475; CVE-2023-27997; CVE-2024-55591; CVE-2024-21887; CVE-2023-4966
Remote Management & Helpdesk	FortiClient EMS, SimpleHelp, PaperCut	CVE-2023-48788; CVE-2024-57727; CVE-2023-27350
Microsoft Servers & Active Directory	Exchange, Windows/AD	CVE-2021-26855; CVE-2020-0688; CVE-2020-1472; CVE-2022-30190
Software Libraries	Apache Log4j	CVE-2021-44228 (Log4Shell)

The concentration of vulnerabilities affecting Fortinet, Ivanti and Citrix products highlights the continued targeting of edge security appliances. These systems are often internet-facing, may lack traditional endpoint detection and response (EDR) coverage, and can fall outside standard patching cycles, making timely remediation particularly important.

FULL FINDINGS

Adversaries With Known Attacks Against The Telecommunications Industry

Adversary Name	Score	Severity	Type	Country
Scattered Spider	81	Critical	Cybercriminal	United States
MuddyWater	80	Critical	Nation-State	Iran
Handala Hack Team	79	Critical	Hacktivist	Iran
Salt Typhoon	78	Critical	Nation-State	China
Volt Typhoon	78	Critical	Nation-State	China
ShinyHunters	77	Critical	Cybercriminal	N/A
Play	75	Critical	Ransomware	N/A
APT28	72	High	Nation-State	Russia
LockBit 5.0	69	High	Ransomware	Russia
Qilin	68	High	Ransomware	Russia
UNC3886	67	High	Nation-State	China
313 Team	67	High	Hacktivist	Iran
DragonForce	65	High	Ransomware	N/A
Medusa	65	High	Ransomware	Russia
Cardinal (Monarch)	65	High	Hacktivist	Russia
Akira	64	High	Ransomware	Russia
UNC1549	63	High	Nation-State	Iran
Warlock	63	High	Ransomware	China
CL0P	60	High	Ransomware	Russia
Flax Typhoon	59	High	Nation-State	China
Liminal Panda	59	High	Nation-State	China
Gallium	58	High	Nation-State	China
INC Ransom	58	High	Ransomware	N/A
APT29	57	High	Nation-State	Russia
NoName057(16)	49	Medium	Hacktivist	Russia
Cyber Islamic Resistance	46	Medium	Hacktivist	Iran
Weaver Ant	45	Medium	Nation-State	China
UNC5537	45	Medium	Cybercriminal	United States
Keymous+	42	Medium	Hacktivist	N/A
FAD Team (Fatimion Cyber Team)	40	Medium	Hacktivist	Iran
Dark Storm Team	37	Medium	Hacktivist	N/A
Russian Legion	27	Medium	Hacktivist	Russia
Hider_Nex	20	Low	Hacktivist	N/A
Nation of Saviors (NOS)	20	Low	Hacktivist	N/A
Sylhet Gang-SG	20	Low	Hacktivist	India

STRENGTHENING YOUR ORGANIZATION THROUGH CYBERSHARE

The cyberthreats outlined in this report are just one example of the intelligence CyberShare participants receive throughout the year. CyberShare helps rural and community-based broadband providers identify, assess and respond to evolving cyberthreats through trusted information sharing, expert analysis and peer collaboration.

Created specifically for small broadband providers, CyberShare delivers actionable threat intelligence, peer-to-peer learning opportunities and direct access to industry and government experts. Today, the program includes more than 150 member companies and 380 individual participants who work together to strengthen the cybersecurity posture of the rural broadband industry.

CYBERSHARE PARTICIPANT BENEFITS

- The CyberShare participant category is for employees of small broadband providers.
- Peer-to-peer information sharing, networking and collaborating
- Daily and weekly report of threats with analysis
- Twice-monthly calls with your peers and/or experts from government or industry
- Listserv and Slack channel for real-time information sharing
- Resources to operate in accordance with the updated NIST Cybersecurity Framework
- Discount on cybersecurity insurance, when available
- Employee cybersecurity training video

In several instances, CyberShare participants learned about serious vulnerabilities impacting their equipment before details were released by manufacturers through the daily threat reports and weekly technical analysis, providing valuable time to assess risks and implement mitigation measures.

CYBERSHARE SUMMIT

Built specifically for rural and small broadband providers, the CyberShare Summit is an opportunity to learn how to get ahead of cyberthreats. The Summit includes government and industry insights, technical overviews and a dynamic mix of technical presentations, small-group discussions and networking opportunities designed to provide practical takeaways attendees can implement as soon as they return to the office. Hosted in partnership with industry associations representing broadband providers across the country, the event creates a unique forum for discussing cybersecurity best practices and the latest threats facing network operators.



CyberShare®

www.cyber-share.org