# TOP 10 CYBER THREATS 2024

**DECEMBER 2024**





# INTRODUCTION

This report provides an in-depth analysis of the top 10 cyber threats that emerged in 2024. The insights presented here draw from a comprehensive study of publicly available threat intelligence and aim to equip cybersecurity professionals with the knowledge necessary to prepare for the challenges of 2025. As the digital landscape continues to evolve and cybercriminals become increasingly sophisticated, understanding these evolving threats is critical to maintaining a robust cybersecurity posture.

2024 proved to be a particularly challenging year in cybersecurity, with incidents arguably surpassing the severity of those observed in 2023. We witnessed mega breaches like the Snowflake incident, which eclipsed the 2023 MOVEit attack in terms of scale and impact. State-sponsored espionage campaigns, notably from China, intensified, posing a greater threat to US interests than in the previous year. Further, destructive campaigns exhibited a concerning growth in both sophistication and recklessness. The CrowdStrike crash served as a stark reminder of the inherent risks associated with over-reliance on a single security vendor, particularly for critical systems. The incidents and trends discussed in this report serve as a call to action for the cybersecurity community.

By understanding these evolving adversarial tactics, techniques, and procedures, we can develop more effective defensive strategies, strengthen our collective resilience, and mitigate the impact of future cyberattacks.

# INDEX

**Data Breaches**

- Snowflake Breach

**Ransomware**

- Dawn of Ransomware
- Iranian State-Sponsored Cybercrime
- North Korean Revenue Generation Campaigns

**Cybercrime Groups**

- Scattered Spider

**Supply-chain Attacks**

- XZ Utils Backdoor
- North Korean Revenue Generation Campaigns

**Espionage Campaigns**

- Russian Espionage Campaigns
- Chinese Telecommunication Hacks

**Disruptive Events**

- Industrial Control System Disruptive Attacks
- CrowdStrike Crash

# Snowflake Breach

# DATA BREACHES

Snowflake is a cloud-based data storage service that allows companies to store massive datasets. In 2024, Snowflake was at the center of a historic data breach campaign that compromised the data of millions of customers across various industries.

The Attack:

- The attackers targeted Snowflake users relying on single-factor authentication.
- They obtained valid login credentials through infostealing malware and used them to access customer databases.
- The breach affected up to 165 Snowflake customers.

The Impact:
The Snowflake campaign had a widespread impact, with stolen data from several major companies being offered for sale on the cybercrime forum BreachForums1. Some of the publicly known impacted organizations include:

- AT&T: 110 million customers impacted
- Santander: 30 million customers impacted
- Ticketmaster: 560 million customers impacted
- Advance Auto Parts: 380 million customers impacted
- LendingTree: 190 million customers impacted

The Perpetrators:
The cybercriminals responsible for the Snowflake Campaign were apprehended by US authorities in November 2024.

Connor Moucka and John Binns were charged for their roles in the attack.
Key Takeaways

- The Snowflake campaign emphasizes the importance of multi-factor authentication (MFA) for all accounts.
- The incident highlights the need to implement robust security measures to detect and prevent data exfiltration, such as egress filtering.
- Organizations should regularly review and monitor traffic to critical systems, like Snowflake, to identify and address suspicious activity.

This incident serves as a reminder for organizations to remain vigilant and proactive in their cybersecurity efforts.

Sources
https://techcrunch.com/2024/06/10/mandiant-hackers-snowflake-stole-significant-volume-data-customers/
https://community.snowflake.com/s/article/Communication-ID-0108977-Additional-Information

# Dawn of Ransomware

# RANSOMWARE

Ransomware attacks continued to plague organizations globally in 2024, with incidents increasing in severity and impact compared to the previous year. The sources highlight two specific ransomware strains: ALPHV/BlackCat and Dark Angels.

They also note the growing collaboration between Iranian state-sponsored cybercriminals and Russian-speaking ransomware affiliates.

**ALPHV/BlackCat:**

- This ransomware gang targeted Change Health, a major US healthcare conglomerate responsible for processing half of all medical claims in the country.
- The attack disrupted pharmacies nationwide, preventing them from filling prescriptions.
- 100 million people were impacted by this attack.
- Change Health paid a ransom of 22 million USD, but the total cost of the attack was estimated between 2.3 billion and 2.45 billion USD. This figure represents one of the highest costs in history for a cyberattack against a single organization.

**Dark Angels:**

- This ransomware gang received the highest ever recorded ransom payment: 75 million USD.
- Cencora, a US pharmaceutical company, reportedly paid this ransom.

**Iranian and Russian Collaboration:**

- The sources reveal a disturbing trend of Iranian state-sponsored cybercriminals collaborating with Russian-speaking ransomware affiliates.
- The Iranian actors gain initial access to networks and then partner with ransomware gangs to encrypt the victim's systems.
- This collaboration allows the Iranian actors to profit from ransomware attacks while potentially maintaining a degree of deniability with their government.
- The US government has been tracking this campaign since 2017.

**Overall Impact:**

- Ransomware attacks continue to pose a significant threat to businesses and critical infrastructure worldwide.
- The increasing collaboration between cybercriminals and nation-state actors underscores the evolving complexity of this threat.
- The financial impact of these attacks is staggering, with ransom payments and recovery costs reaching record highs.

**Mitigating the Threat:**

- Organizations must prioritize implementing robust cybersecurity measures to defend against ransomware attacks.

These measures should include:

- Multi-factor authentication (MFA)
- Regular security awareness training for employees
- Strong endpoint detection and response (EDR) solutions
- Robust data backup and recovery plans
- Incident response planning

Sources
https://therecord.media/prescriptions-nationwide-impacted-by-change-healthcare-incident

# Iranian State-Sponsored Cybercrime

# RANSOMWARE

In 2024, US authorities revealed that Iranian government-backed cybercriminals have been collaborating with Russian-speaking ransomware affiliates to attack companies worldwide. These cybercriminals have been active since at least 2017, gaining access to networks and then working with ransomware affiliates to encrypt victim networks in exchange for a cut of the ransom.1 The US authorities did not state whether Iranian officials were aware of or approved of the ransomware activity.

**The Iranian Actors:**

- These cybercriminals are known by many names: Pioneer Kitten, Fox Kitten, UNC757, Parisite, RUBIDIUM, and Lemon Sandstorm.
- They are linked to an Iranian company named Danesh Novin Sahand, which likely serves as an IT front company for their operations.

**Modus Operandi:**

- In 2023, they created a persona called "Br0k3r" on Russian-speaking cybercriminal forums.
- "Br0k3r" advertised access to compromised networks for sale on a Tor site called "Br0k3r's Shop."
- They have reportedly collaborated directly with ransomware affiliates, including NoEscape, RansomHouse, and ALPHV/BlackCat.
- They often hide their Iranian origins from their ransomware partners, remaining intentionally vague about their nationality.

**Motives:**

- These Iranian actors are likely stealing sensitive information from the networks they compromise and providing it to the Iranian government.2
- The ransomware attacks may not be officially sanctioned, as the actors have reportedly expressed concern about the Iranian government monitoring their cryptocurrency transactions associated with these activities.2

**Connections to Past Campaigns:**

These same actors have been linked to hack-and-leak campaigns targeting Israeli companies, such as the Pay2Key attacks in late 2020.3
The collaborative activities of Iranian state-sponsored actors and ransomware gangs represent a growing and complex cyber threat.

The Iranian government benefits from intelligence gathering and potential financial gains, while maintaining a degree of deniability. This highlights the increasing convergence of cyber espionage and financially motivated cybercrime.

Sources
https://attack.mitre.org/groups/G0117/

# North Korean Revenue Generation Campaign

# RANSOMWARE

Cyber operations by the Democratic People's Republic of Korea (DPRK), also known as North Korea, were highly active throughout 2024, showing no signs of slowing down. Their focus remains on revenue generation operations to evade international sanctions and fund the regime. These campaigns involve various tactics:

**Cryptocurrency Theft:**

- The United Nations is investigating 58 cyberattacks attributed to North Korean hackers, involving the theft of 3 billion USD over a six-year span.1
- Cryptocurrency investigator ZachXBT revealed research into over 25 North Korean campaigns between 2020 and 2023, which resulted in the theft of a combined 200 million USD.1

**Software Supply Chain Attacks:**

- North Korean adversaries have been targeting the open source software ecosystem by poisoning Python and NPM packages to deliver malware to software developers.1 This tactic allows them to wait for victims to download the compromised packages, similar to malvertising and watering hole attacks.

**Remote IT Worker Campaigns:**

- North Korea has been employing a tactic of tricking American and British businesses into hiring remote IT workers to earn salaries and evade sanctions.
- These workers have reportedly earned hundreds of thousands of dollars each, collectively generating hundreds of millions of dollars annually.
- Thousands of North Korean IT workers have also been sent abroad, primarily to China and Russia.

Ransomware Attacks:

- North Korean state-sponsored ransomware campaigns appear to have escalated in 2024.
- Security researchers have uncovered links between North Korean hacking groups and various ransomware families, including PLAY, Maui, and H0lyGh0st.

These activities demonstrate North Korea's ongoing commitment to leveraging cyber operations for financial gain. Their tactics are evolving and becoming increasingly sophisticated, posing a significant threat to businesses and organizations worldwide.

Sources
https://www.ncsc.gov.uk/news/uk-republic-of-korea-issue-warning-dprk-state-linked-cyber-actors-attacking-software-supply-chains
https://www.justice.gov/opa/pr/justice-department-disrupts-north-korean-remote-it-worker-fraud-schemes-through-charges-and

# Scattered Spider

# CYBERCRIME GROUPS

Scattered Spider is one of the largest English-speaking cybercriminal groups. They operate more like a community rather than a close-knit group of individuals. Their attacks have become increasingly notorious since 2022, targeting companies like Twilio, Reddit, Coinbase, MGM, and Caesars. Several Scattered Spider members were caught and arrested in 2024.

Key Activities:

- Transport for London (TfL) Attack: In September 2024, Scattered Spider attacked TfL, impacting customer data, payment processing systems, and live data feeds. The attack forced TfL to reset the passwords of 30,000 employees in person and implement identity verification checks for system access.
- MGM Attack: A 17-year-old from Walsall, UK, was arrested in connection with both the TfL and MGM attacks, both of which were attributed to Scattered Spider.
- Arrests and Charges: Following these arrests, five more Scattered Spider members (four from the US and one from the UK) were charged by the US Department of Justice.

Group Structure:

- Despite the arrests, Scattered Spider remains a significant threat. The FBI estimates that the group comprises approximately 1,000 individuals.

Scattered Spider's large membership and community-based structure make it difficult to completely dismantle. Law enforcement agencies have had some success in apprehending certain members, but the group's activities are expected to persist.

Sources
https://tfl.gov.uk/campaign/cyber-security-incident

# XZ Utils Backdoor

# SUPPLY-CHAIN ATTACKS

In March 2024, a malicious backdoor was discovered in XZ Utils, a widely used data compression software library. This backdoor, tracked as CVE-2024-3094, was given a critical CVSS score of 10/10. It affected several Linux distributions, including Fedora, Debian Unstable, and Kali Linux. The incident was a sophisticated, multi-year supply-chain attack targeting an open-source code repository.

**The Attacker:**

- The individual behind the attack is known as Jia Tan.
- Little is known about Jia Tan's true identity or their location.
- Their online presence appears to be a single-purpose invented persona created solely for this campaign.

**Modus Operandi:**

- Jia Tan spent two years volunteering to write code for XZ Utils and other open-source software projects.
- They made over 6,000 code changes to at least seven projects between 2021 and February 2024, gradually gaining trust and influence.
- By January 2023, Jia Tan’s malicious code started being integrated into XZ Utils.
- Over the following year, they effectively took control of the project from the original maintainer.

**Backdoor Functionality:**

- The backdoor was designed to alter the operation of OpenSSH server daemons and interfere with authentication in sshd.
- It would allow unauthorized remote access to affected systems.
- The backdoor did not "call home" but instead waited for the attacker to connect to the target machine via SSH and authenticate with a private key.

**Discovery and Impact:**

- Fortunately, the backdoor was caught early enough by security researcher Andres Freund, preventing widespread exploitation.
- The backdoor primarily affected bleeding-edge Linux distributions that had immediately incorporated the latest versions of XZ Utils.

**Attribution and Implications:**

- The patience and complexity of the attack suggest that Jia Tan's activities may have been part of a long-running state-sponsored campaign.
- The lack of any other online presence linked to Jia Tan further supports this theory.
- The incident highlights the risks associated with incorporating third-party software without thorough code integrity verification.

The XZ Utils backdoor incident serves as a stark reminder of the increasing sophistication and persistence of nation-state actors targeting open-source software projects. It underscores the importance of robust security measures and vigilance within the open-source community.

Sources
https://www.theregister.com/2024/03/29/malicious_backdoor_xz/

# Russian Espionage Campaign

# ESPIONAGE CAMPAIGNS

Bold Russian Espionage Campaign Update
Throughout 2024, Russia continued to conduct bold cyber-espionage campaigns, primarily targeting Ukrainian and NATO member state government entities and technology companies that provide services to government and military networks.

These campaigns involved well-known Russian state-sponsored advanced persistent threat (APT) groups.

**Key Actors and Activities:**

- **COZY BEAR (APT29 or Midnight Blizzard)**:
  - Associated with the Russian Foreign Intelligence Service (SVR).
  - Breached Microsoft's corporate email system in January 2024, starting with password spraying against a legacy test account.
  - Engaged in a spear-phishing campaign using .RDP configuration files as email attachments in October 2024.
- **FANCY BEAR (APT28 or Forest Blizzard)**:
  - Linked to the Russian military Intelligence agency (GRU).
  - Conducted a "nearest neighbor attack" against a US-based entity, compromising a nearby WiFi network to breach their intended target.
- **EMBER BEAR (Cadet Blizzard)**:
  - A relatively new GRU group.
  - Primarily targets Ukrainian government and telecommunication entities but has also targeted critical national infrastructure (CNI) organizations across Europe and the Americas.

**Key Observations:**

- Persistence: Russian APT groups continue to demonstrate persistence in targeting organizations of strategic importance.
- Sophistication: The tactics used by these groups, such as the "nearest neighbor attack", highlight their increasing sophistication and willingness to employ unconventional methods.
- Expansion of Targets: While Ukraine and NATO members remain primary targets, Russian APT groups have expanded their focus to include CNI organizations in other regions.

The activities of these Russian APT groups highlight the ongoing cyber threat posed by Russia. Their boldness and sophistication underscore the need for robust cybersecurity defenses and vigilance against state-sponsored espionage activities.

Sources
https://attack.mitre.org/groups/G0016/
https://msrc.microsoft.com/blog/2024/01/microsoft-actions-following-attack-by-nation-state-actor-midnight-blizzard/
https://www.volexity.com/blog/2024/11/22/the-nearest-neighbor-attack-how-a-russian-apt-weaponized-nearby-wi-fi-networks-for-covert-access/

# Chinese Telecommunication Hacks

# ESPIONAGE CAMPAIGNS

Throughout 2024, Chinese APT groups were attributed to several significant intrusion campaigns, specifically targeting the telecommunications sector globally.

**Key Actors and Activities:**

- **Salt Typhoon:**
  - A new China-nexus APT group.
  - Compromised multiple US telco firms, including Verizon, AT&T, Lumen, and T-Mobile.
  - The breaches allegedly enabled snooping on downstream targets, including US law enforcement wiretapping systems and US presidential campaigns.
- **Volt Typhoon:**
  - Had its botnet of compromised SOHO routers taken down by US law enforcement in early 2024.
  - Rebuilt the botnet by November 2024.
  - Reportedly breached Singapore Telecommunications (Singtel) in mid-2024.
- **LIMINAL PANDA**
  - Another China-nexus threat group that targets telco technology.
  - Possesses an extensive understanding of interconnections between telco providers, GSM protocols, and targeted mobile subscriber information, call metadata, and SMS messages.

**Other Notable Activities:**

- **Leaks from I-SOON:**
  - A Chinese Ministry of Public Security (MPS) contractor specializing in network penetration research.
  - Leaked data provided insights into how the Chinese MPS operates, using Chinese commercial surveillance vendors, and their technical capabilities.
- **Sophos' Pacific Rim Report:**
  - Revealed details about a five-year counter-offensive operation against a Chinese exploit development unit.

**Key Observations:**

- Focus on Telecommunications: Chinese APT groups have demonstrated a clear focus on targeting telecommunications companies globally.
- Strategic Espionage: The targeting of US law enforcement wiretapping systems and presidential campaigns suggests a strategic espionage motive behind these attacks.
- Technical Expertise: The groups involved exhibit a high level of technical expertise and understanding of telecommunications infrastructure and protocols.

These activities highlight the significant cyber threat posed by Chinese APT groups to the global telecommunications sector. Their focus on strategic espionage and sophisticated tactics underscore the need for heightened vigilance and robust security measures within the industry.

Sources
https://archive.ph/YwAjw
https://www.theregister.com/2024/10/07/verizon_att_lumen_salt_typhoon/

# ICS Disruptive Attacks Update

# SUPPLY-CHAIN ATTACKS

2024 saw several disruptive attacks on industrial control systems (ICS). These attacks, often attributed to hacktivist groups, targeted critical infrastructure in the US and Europe, demonstrating increasing brazenness and concerning potential for real-world impact.

**Key Actors and Activities:**

- **Cyber Army of Russia Reborn (CARR):**
  - A hacktivist group that has taken credit for targeting ICS of US and European water and hydroelectric utilities at least three times.
  - Posted videos to Telegram showcasing their manipulation of human-machine interfaces (HMIs).
  - Targeted victims include:
    - Multiple US water utilities in Texas.
    - A Polish wastewater treatment plant.
    - A small French water mill (which the hackers claimed was a hydroelectric dam).
  - Mandiant linked CARR to Sandworm, a GRU unit notorious for targeting Ukrainian ICS.
  - Connections between CARR and Sandworm:
    - Google found CARR's YouTube accounts were accessed from an IP address controlled by Sandworm.
    - Stolen data from Sandworm attacks on Ukrainian targets was posted to CARR's Telegram account.
  - Mandiant believes the Russian GRU is likely involved in creating and running CARR.
  - In July 2024, the US Treasury sanctioned two CARR members.
- **FrostyGoop:**
  - Malware discovered by Dragos in April 2024, targeting ICS in Ukraine.
  - Used in an attack against a Ukrainian municipal district energy company, causing a two-day heating system disruption to over 600 apartment buildings.
  - Notable as the latest ICS malware to achieve real-world impact and the first to do so by manipulating the ModbusTCP protocol.
  - Poses a significant threat to various CNI sectors due to ModbusTCP's wide adoption.
  - Operates by issuing ModbusTCP commands directly from the attacker's infrastructure, eliminating the need to place malware on the targeted network, making detection and forensics more difficult.

**Key Observations:**

- Increased Real-World Impact: ICS attacks in 2024 demonstrated a concerning shift towards causing real-world disruption and impacting critical infrastructure.
- Hacktivist Involvement: Hacktivist groups like CARR have entered the ICS attack landscape, potentially increasing the risk of unpredictable and disruptive actions.
- Sophistication and Innovation: FrostyGoop's use of ModbusTCP and its ability to operate without placing malware on target networks highlights the increasing sophistication and innovation in ICS malware development.

The disruptive ICS attacks observed in 2024 underscore the growing threat to critical infrastructure from both state-sponsored actors and hacktivist groups.

Sources
https://www.wired.com/story/cyber-army-of-russia-reborn-sandworm-us-cyberattacks/

# CrowdStrike Crash

# DISRUPTIVE EVENTS

The CrowdStrike Crash, also referred to as WannaStrike or the Blue Falcon of Death, was the single event with the highest global impact in 2024. While not a cyberattack, it triggered a cascading disruptive event caused by CrowdStrike's endpoint detection and response (EDR) software for Windows. The crash primarily affected North American and European countries where most of CrowdStrike's customers are located.

**Key Details:**

- The issue stemmed from a failure to adequately test patches before deployment, leading to a widespread system failure.
- The incident highlighted the over-reliance on a single piece of software for critical security functions. CrowdStrike's software became a single point of failure for many organizations.

**Impact and Implications:**

- The crash caused major disruptions to businesses and organizations worldwide, as their systems were left unprotected.
- The event raised significant concerns about operational resilience, supply chain security, and incident response capabilities, areas emphasized by cybersecurity frameworks like the European Union's NIS2 Directive and DORA Regulation.
- The CrowdStrike crash will likely have long-term consequences for how organizations implement changes to meet these regulatory requirements.

**Exploitation by Cybercriminals:**

- In the aftermath of the crash, cybercriminals exploited the situation by launching phishing campaigns, registering malicious domains, and distributing malware disguised as CrowdStrike support.
- These malicious activities aimed to capitalize on the IT disruptions and target vulnerable organizations during the recovery period.

**Key Takeaways:**

- The CrowdStrike Crash underscores the importance of thorough patch testing and the need to avoid over-reliance on single security vendors for critical systems.
- Organizations should prioritize building robust operational resilience and implementing comprehensive incident response plans to mitigate the impact of similar events in the future.
- The incident serves as a reminder of the opportunistic nature of cybercriminals who quickly exploit vulnerabilities and leverage major incidents to their advantage.

Sources
https://www.bbc.co.uk/news/articles/cp4wnrxqlewo
https://www.theregister.com/2024/07/19/cyber_criminals_quickly_exploit_crowdstrike/

# TOP 10 CYBER THREATS 2024

**DECEMBER 2024**

thecybersecurity.club

Stay Ahead of Threats Unlock Global Cybersecurity Insights and Intelligence.

Join a global community of cybersecurity professionals, you'll gain valuable insights, intelligence briefings, and in-depth research reports.

The Cybersecurity Club keeps you updated on the latest industry trends and emerging threats, helping your organization make informed security decisions.

With timely and actionable intelligence, you'll be able to proactively strengthen your security defenses and stay ahead of potential risks.