

# Akira Ransomware Gang: A Rising Threat to Global Enterprises

The Akira Ransomware Gang has quickly become a big threat to businesses and organizations, showing a high level of skill and harmful intentions. This article digs into who they are, where they target, what security holes they exploit, which industries they go after, and some of their latest bad actions.

## Who Are They?

The Akira gang is suspected to have affiliations with the now-defunct Conti ransomware gang, inheriting a legacy of ransomware expertise from one of the most notorious cybercrime entities. Their operations bear the hallmark of a double extortion model, where they first exfiltrate sensitive data before deploying their ransomware to encrypt files. Victims are coerced to pay a ransom for decryption keys and to prevent the public leakage of their stolen data. The group has claimed over 100+ victims, which have typically ranged in the small- to medium-size business scale.

## Targeted Regions:

The Akira Ransomware Gang seems to have a particular focus on North America, especially targeting entities in the United States and Canada. These regions have experienced a higher number of attacks from this gang compared to others. The reasons behind this geographical focus could be varied. It might be due to the presence of more lucrative targets, such as large corporations or critical infrastructure, which can afford to pay hefty ransoms.

## CVEs Exploited:

The Akira ransomware was discovered exploiting a zero-day vulnerability, labeled as **CVE-2023-20269**. This vulnerability resides in the remote access VPN feature of Cisco's Adaptive Security Appliance (ASA) and Firepower Threat Defense (FTD) software. It holds a CVSS score of 5.0, categorizing it as a medium severity threat.

The primary targets of Akira ransomware are Cisco ASA VPNs, particularly those lacking multifactor authentication. The exploitation of the CVE-2023-20269 vulnerability serves as the entry point in the infection chain, allowing the malicious software to infiltrate the targeted systems.

## Targeted Industries:

The Akira Ransomware Gang is casting a wide net across various sectors. Key targets include education, healthcare, energy, real estate, and manufacturing. They've also extended their malicious reach to finance, engineering, legal, and technology sectors. Government entities, logistics, retail, construction, and even non-profit organizations aren't spared. Their diversified targeting underscores a critical need for bolstered cybersecurity across all sectors.

## Latest Attacks:

Based on the extensive list of attacks carried out by the Akira Ransomware Gang, it's evident that no sector is safe. Here are some notable incidents from various sectors, indicating the widespread nature of their malicious activities:

- **Educational Institutions Targeted:** On October 27, 2023, Stanford University fell victim to Akira's nefarious actions. Similarly, Mercer University and Morehead State University were targeted on May 9, and July 27, 2023, respectively.
- **Healthcare Sector Alert:** The Royal College of Physicians and Surgeons of Glasgow faced an attack on October 20, 2023, showcasing the continued threat to healthcare institutions.
- **Energy Sector Breach:** BHI Energy experienced a significant data breach on an undisclosed date, highlighting the vulnerabilities within the energy sector.
- **Manufacturing Mayhem:** Companies like Accuride and A123 Systems were attacked on September 12, and July 11, 2023, reflecting the risks faced by manufacturing entities.

## MITRE ATT&CK® Techniques:

| Tactic    | Technique ID   | Technique Name   |
|-----------|----------------|--|
| Execution | T1204          | User Execution   |
| Discovery | T1082<br>T1083 | System Information Discovery<br>File and Directory Discovery |

|        |  |  |
|--------|--|--|
| Impact | <a href="#">T1486</a><br><a href="#">T1490</a> | Data Encrypted for Impact<br>Inhibit System Recovery |
|--------|--|--|

# Conclusion:

The actions of the Akira Ransomware Gang show a growing danger where no industry is safe. Their mix of technical skill, a wide range of targets, and high money demands make Akira a big threat in the cyber world. Being aware, having strong cyber protection, and working together across different industries are key to stopping the harm caused by such bad actors.

---

Revision #1  
Created 27 October 2023 12:37:54 by Admin  
Updated 27 October 2023 13:49:15 by Admin