

Threat Actors

- [Lazarus](#)
- [Akira Ransomware Gang: A Rising Threat to Global Enterprises](#)

Lazarus

download.png

Image not found or type unknown

Introduction

Lazarus, also known as Hidden Cobra or Zinc, is a **North Korean state-sponsored hacking group** that has been active since 2009. The group is one of the world's most active threat actors and has been behind large-scale cyber-espionage and ransomware campaigns. Lazarus has often switched targets through time, probably according to nation-state interests.

Lazarus is responsible for infamous cyber incidents such as the attack on Sony Pictures in 2014 and the spread of the WannaCry ransomware in 2017 . The group has also been spotted attacking the defense industry and cryptocurrency markets. Lazarus is known for its involvement in several high-profile bank heists. The group has also targeted energy providers in the U.S., Canada, and Japan with a new malware arsenal .

Also Known As

"Operation DarkSeoul", "Dark Seoul", "Hidden Cobra", "Hastati Group", "Andariel", "Unit 121", "Bureau 121", "NewRomanic Cyber Army Team", "Bluenoroff", "Subgroup: Bluenoroff", "Group 77", "Labyrinth Chollima", "Operation Troy", "Operation GhostSecret", "Operation AppleJeus", "APT38", "APT 38", "Stardust Chollima", "Whois Hacking Team", "Zinc", "Appleworm", "Nickel Academy", "APT-C-26", "NICKEL GLADSTONE", "COVELLITE", "ATK3", "G0032", "ATK117", "G0082"

Region Focus

1. South Korea
2. Bangladesh Bank
3. Sony Pictures Entertainment
4. United States
5. Thailand
6. France

7. China
8. Hong Kong
9. United Kingdom
10. Guatemala
11. Canada
12. Bangladesh
13. Japan
14. India
15. Germany
16. Brazil
17. Thailand
18. Australia
19. Cryptocurrency exchanges in South Korea

Technology

Lazarus has used a variety of techniques to carry out its attacks. The group has been involved in large-scale cyberespionage campaigns, ransomware campaigns, and even attacks against the cryptocurrency market. Lazarus has also been observed using the MATA malware framework to target various industries for cybercrime purposes, such as stealing customer databases and spreading ransomware .

Techniques

The disruptive operations performed by Lazarus involve DDOS attacks and Wipers with time-based triggers. These include KILLMBR with a hard-coded wiping date, and QDDOS, which has duration date that wipes data ten days after infection. DESTOVER, a backdoor equipped with wiping capabilities, is another .

CVEs Focus

- CVE-2021-21551: A vulnerability in a Dell driver that allows user-mode applications to read and write kernel memory. The Lazarus Group used this vulnerability to bypass security solutions and execute malicious code²
- CVE-2017-0199: A vulnerability in Microsoft Office that allows remote code execution via specially crafted files. The Lazarus Group used this vulnerability to deliver malware to their targets via phishing emails.

- CVE-2017-11882: A vulnerability in Microsoft Office that allows arbitrary code execution via a maliciously modified equation editor. The Lazarus Group used this vulnerability to deliver malware to their targets via phishing emails.
- CVE-2018-4878: A vulnerability in Adobe Flash Player that allows remote code execution via a specially crafted SWF file. The Lazarus Group used this vulnerability to deliver malware to their targets via phishing emails or compromised websites.

Industry Attacked

Lazarus has attacked various industries such as automotive, academic, defense sectors in Eastern Europe and other parts of the world . The group has also targeted financial institutions and energy providers in the U.S., Canada, and Japan.

Reference

1. <https://github.com/MISP/misp-galaxy/blob/main/clusters/threat-actor.json>

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 T1083	System Information Discovery File and Directory Discovery

Impact	T1486 T1490	Data Encrypted for Impact 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.