Sondos Farrah
1200905

# Recent Cybersecurity Incidents and Vulnerabilities

## ALPHV/BlackCat Ransomware Targeting Healthcare Sector

In early 2024, the FBI, CISA, and the Department of Health and Human Services (HHS) issued a warning to U.S. healthcare organizations regarding a significant increase in ALPHV/BlackCat ransomware attacks. This surge, beginning in mid-December 2023, primarily targeted hospitals and healthcare facilities. The ALPHV/BlackCat ransomware, also known as RaaS (Ransomware as a Service), has evolved with its 2.0 Sphynx update, which includes enhanced defense evasion capabilities and the ability to target both Windows and Linux systems, including VMware instances. The increase in attacks is believed to be a response to law enforcement actions against the group. The advisory urged healthcare organizations to implement recommended mitigations to protect against these sophisticated threats.

## Ivanti SSRF Vulnerability Exploitation

In early February 2024, cybersecurity experts highlighted a surge in attacks exploiting a server-side request forgery (SSRF) vulnerability in Ivanti's Connect Secure and Policy Secure solutions. The vulnerability, tracked as CVE-2024-21893, allows authenticated attackers to access restricted resources. Ivanti disclosed the flaw along with another high-severity vulnerability, CVE-2024-21888. The SSRF vulnerability has been actively exploited in the wild, with the situation expected to evolve as threat actors adapt their tactics. Ivanti has provided temporary workarounds and continues to update its guidance as more information becomes available.

## Attack on MGM Resorts

In September 2023, MGM Resorts suffered a significant cyberattack that disrupted operations across its properties. The attack, attributed to the ALPHV/BlackCat ransomware group, led to the shutdown of reservation systems, digital keys, and some slot machines. The attackers reportedly used social engineering techniques to gain access to MGM's network, highlighting the persistent threat of sophisticated ransomware operations. The incident underscores the need for robust cybersecurity measures and employee training to mitigate social engineering risks. The attack on MGM Resorts is part of a broader trend of ransomware groups targeting high-profile organizations for substantial ransoms.

## Reference

https://securityaffairs.com/