# TLP WHITE: Threat Intel Report: Ransomware Groups Targeting Hospitals

This report consolidates information on notable ransomware groups targeting hospitals, their tactics, techniques, and procedures (TTPs), and provides indicators of compromise (IOCs) to aid in detection and prevention efforts.

**Rhysida Group**

TTPs: The Rhysida Group is known for leveraging external-facing remote services to gain initial access and persist within networks. Their mitigation strategies include requiring phishing-resistant multi-factor authentication (MFA) across all services, especially critical systems, and implementing enhanced logging and restrictions on command-line and scripting activities.

Mitigation Strategies: Recommendations include disabling unnecessary command-line and scripting activities, restricting PowerShell use, updating PowerShell to the latest version, and securing remote access tools.

IOC’s and TTP’s for this actor group from CISA

**ALPHV Blackcat**

Overview: In February 2023, the ALPHV Blackcat group announced an update known as Ransomware 2.0 Sphynx, enhancing their affiliates' capabilities, including better defense evasion and additional tooling. This group has compromised over 1000 entities, with demands exceeding $500 million, and actual payments nearing $300 million.

Mitigation Recommendations: Key strategies involve taking inventory of assets, prioritizing the remediation of known vulnerabilities, enforcing multifactor authentication, and eliminating unnecessary ports and applications.

IOC’s and TTP’s for ALPHV / BLACKCAT from CISA

**Daixin Team**

TTPs: The Daixin Team employs a variety of methods for persistence, credential access, lateral movement, and exfiltration, including account manipulation, credential dumping, and the use of SSH and RDP for lateral movement. They've been observed using tools like Ngrok for data exfiltration.

IOCs: Specific SHA256 hashes associated with Daixin Team's tools have been identified, providing a means for detection.

Mitigation Strategies: Installing updates for systems and software as soon as they are released, securing and monitoring Remote Desktop Protocol (RDP), implementing user training programs, and requiring MFA for critical services are among the recommended actions.

IOC’s and TTP’s for DAIXIN TEAM from CISA

## Conclusion

The evolution of ransomware targeting the healthcare sector underscores the necessity for robust cybersecurity defenses. Healthcare organizations are encouraged to implement the recommended mitigation strategies and stay vigilant against the TTPs and IOCs associated with these ransomware groups to protect sensitive data and critical healthcare infrastructure.