CYBER SECURITY OPERATION CENTRE (CSOC), ODISHA

Document Type	**Advisory**
Brief Description	Guidance on an ongoing Hactivist operation #OpsPatuk conducted by the Malaysian Hactivist threat group dubbed 'DragonForce'; in relation to the recent controversy in the name of Prophet Mohammad
Description of Threat	#OpsPatuk aka Operation Patuk is an ongoing operation led by a Malaysia-based hacktivist group dubbed 'DragonForce'. On June 6, 2022, witnessed one of the first activities by the group in association with the operation. The operation is in target towards government websites and infrastructures DragonForce and its supporters have predominantly targeting victims using the following techniques: DDoS Website Defacement Compromising VPN Portals with stolen credentials Targeting the web application vulnerabilities Exploiting recent Atlassian Confluence vulnerability CVE-2022-26134 Over 100+ Indian websites are targeted by the group. The group has been reported to be targeting mainly Government, Technology, Financial Services, Manufacturing and Education sectors.
Impact Assessment	These are the possible attacks they can conduct. • DDoS Attacks: DDoS attack may take place. The effects of DDoS attacks are website downtime, server and hosting issues, website vulnerability. • Public Exploits: It is an attack on a computer system, especially one that takes advantage of a particular vulnerability the system offers to intruders • Leaked Credentials: - Related to Atlassian Confluence RCE vulnerability (CVE-2022-26134)
Recommendation	• Secure APIs by evaluating the sensitive data and resources they're exposing • Organizations must do hardening and security/vulnerability testing of their web applications as well as network • Ensure all internal communications are encrypted for applications • Organizations have to install WAFs that are designed to examine and monitor incoming traffic for blocking any attack attempts. WAFs offer the best way of compensating for code sanitization deficiencies. • organizations should also be aware of other malicious web application vulnerabilities such as insecure cryptography, insufficient logging and monitoring, and using components with known vulnerabilities.