

Advisory on Cyber Threats from Chinese Government-linked Actors



Chinese government-linked cyber actors are employing a mix of automated tools and manual techniques to compromise sensitive data across various sectors globally. Organizations are advised to enhance their cybersecurity measures to mitigate these threats.

- Cyber actors are using automated scanning tools and botnets.
- They exploit vulnerabilities in systems like Microsoft Exchange.
- Persistent access is achieved through VPN software.
- Organizations are urged to implement multifactor authentication.
- Timely patching of systems is critical to reduce risks.

Overview

Chinese government-linked cyber threat actors are leveraging a combination of automated tools and hands-on techniques to target sensitive data. These activities have been observed across various sectors, including critical infrastructure.

Techniques Used

The actors utilize automated scanning tools and large-scale botnets to identify vulnerabilities. They exploit weaknesses in systems, particularly through cross-site scripting attacks and password spraying on Microsoft Exchange servers. Persistence is maintained via VPN software, allowing for the exfiltration of sensitive information such as emails and credentials.

Recommended Actions

To mitigate the risks associated with these cyber threats, organizations should take proactive measures. It is essential to disable any unused services and ports, sanitize web application inputs to prevent injection attacks, and implement multifactor authentication for all services. Additionally, applying timely patches to systems will help reduce the likelihood of compromise.

What to do now

1. Disable unused services and ports.
2. Sanitize web application inputs.
3. Implement multifactor authentication for all services.
4. Apply timely patches to systems.