



Volt Typhoon

Source: [IE](#)

Microsoft has detected covert, targeted malicious activity by the [Chinese state-sponsored group Volt Typhoon](#), aimed at **post-compromise credential access & network system discovery**, targeting US [critical infrastructure](#).

- Volt Typhoon affecting various sectors including [communications](#), [manufacturing](#), utilities, transportation, construction, maritime, government, IT, and education.
 - Observed behaviour indicates a **covert intent** for prolonged undetected espionage and access retention.
 - To reach their goal, the attacker **focuses on stealth**, using basic techniques to collect data and maintain access, while disguising their activity within regular network traffic, often through compromised home office equipment and custom tools for remote control.
- **Equation Group (USA)**, [Fancy Bear \(Russia\)](#), [APT37 \(North Korea\)](#), [Turla \(APT34\) \(Iran\)](#), [SandWorm \(Russia\)](#), etc. are some of the other hacking groups used by security agencies.

Read More: [Cyber Security](#)

PDF Reference URL: <https://www.drishtias.com/printpdf/volt-typhoon>