Mustang Panda



|  |
| --- |
| Buff:  +2 SOPH (INT) | +1 RES (CON) |

|  |  |  |
| --- | --- | --- |
| Techniques:   * Encrypt exfiltrated data and C2 communication to evade detection. * Automate collection of information on a system through custom scripts and programs. * Uses USBs to exfiltrate data and infiltrate air-gapped networks. * Uses extensively PlugX, a remote access trojan tool. | Motivations:   * The motivations of the Chinese government * Seeking government trade secrets * Targets government entities, nonprofits, religious, and other non-governmental organizations in the U.S., Europe, Mongolia, Myanmar, Pakistan, and Vietnam, among others | Past Attacks:   * Targeted the Vatican and the Catholic Church (2021). * Target the ruling Communist party of Vietnam through spear-phishing campaigns (2017). * During the Russian-Ukranian war, targets refugee organizations and other humanitarian European efforts (2022). |