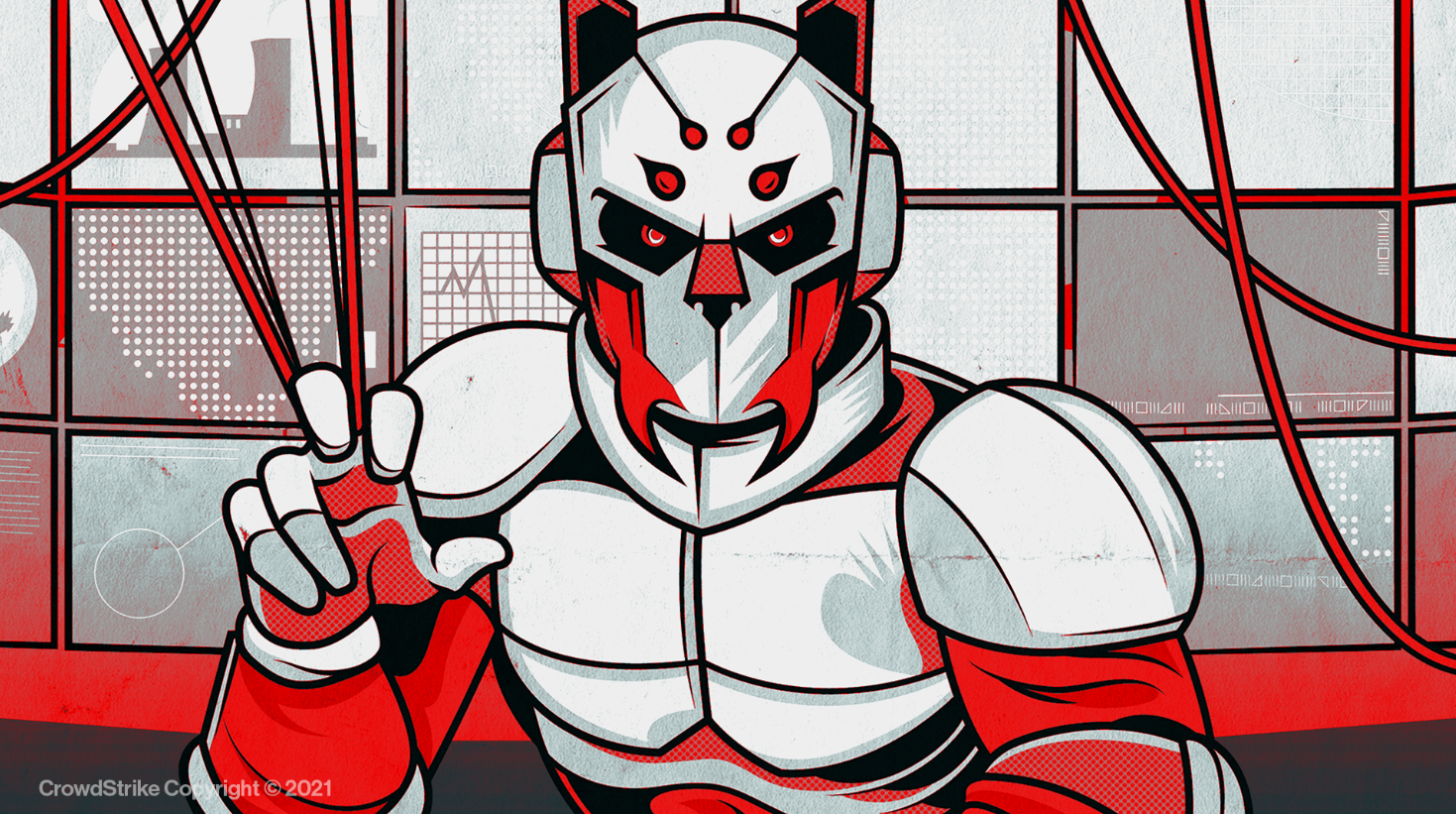
Wicked Panda



|  |
| --- |
| Buff:  +1 COMP (DEX) | +1 RES (WIS) | +1 CHA |

|  |  |  |
| --- | --- | --- |
| Techniques:   * Removes artifacts of the exploitation and damage done to the system to avoid detection. * Dumps user account hashes to move laterally across the network. * Signs malware as legitimate files. * Installs crypto-miners on victim systems. | Motivations:   * The motivations of the Chinese government. * Seeks financial gain * Targets Healthcare, Telecom, Technology, and Video Game Industries in over 14 countries. | Past Attacks:   * Attacked multiple airlines in a coordinated supply-chain compromise (2021) * Deployed malware that monitored and saved SMS conversations on specific phone numbers (2019). * In a global attack, the group targeted over 75 companies with the same few exploits (2020). |