Labyrinth Chollima



|  |
| --- |
| Buff:  +2 RES (CON) | +1 CHA |

|  |  |  |
| --- | --- | --- |
| Techniques:   * Employs keyloggers to harvest credentials. * Encodes exfiltration or code with simple XOR or base64 ciphers. * Overwrites individual files or complete disk drives, rendering the information unusable. * Creates fake social media profiles and email addresses to social engineer victims. | Motivations:   * The motivations of the North Korean government. * Obtaining government secrets from other countries. * Seek financial profits. * Propagate positive views of the North Korean government. * Destroy/wipe system infrastructure of adversaries | Past Attacks:   * Destructive wiper attack against Sony Pictures Entertainment (2014). * Stole $16 million from multiple banks (2015). * Massive DDoS attacks against US and South Korean sites (2009). |