Remix Kitten



|  |
| --- |
| Buff:  +2 COMP (DEX) | +1 CHA |

|  |  |  |
| --- | --- | --- |
| Techniques:   * SQL injection for initial compromise. * Customizes and uses Mimikatz to steal system credentials. * Moves laterally in a compromised network through SMB, SSH, and RDP. * Uses HTTP and DNS for C2 traffic. * Uses a front company-- Rana Intelligence Computing-- in their operations | Motivations:   * Motivations of the Iranian Ministry of Intelligence and Security (MOIS). * Seeks diplomatic and strategic information from other governments. * Targeted the travel, hospitality, academic, and telecommunications industries in Iran and across Asia, Africa, Europe, and North America. | Past Attacks:   * Mass theft of personal information which an emphasis on telecommunication industries in the Middle East (2019). * Deployed malware to spy on Iran-based foreign diplomatic entities (2019). |