Ocean Buffalo



|  |
| --- |
| Buff:  +1 SOPH (INT) | +2 COMP (DEX) |

|  |  |  |
| --- | --- | --- |
| Techniques:   * Uses PowerShell for exploitation, reconnaissance, and evasion. * Masquerades malicious software as legitimate installers, or injects malware into system dll’s. * Extensively uses strategic web compromises to compromise victims. * Once compromised, enumerates system ports, interfaces, users, and systems. | Motivations:   * The motivations of the Vietnamese government. * Spies and performs surveillance on activists, journalists, and bloggers. * Targets private industries, foreign governments, media organizations, and research institutes. | Past Attacks:   * Deployed spyware on Vietnamese Human Rights activists (2021). * Installed MacOS backdoor through macros in a Word document spread through a phishing attack. (2018). * Sent phishing emails to Wuhan and Chinese government officials at the beginning of the COVID-19 crisis in order to gather system types, hostnames, valid email addresses, and network information. |