Venomous Bear



|  |
| --- |
| Buff:  +3 DEADL (STR) |

|  |  |  |
| --- | --- | --- |
| Techniques:   * Develops their own malware, execution scripts, and personally customizes well-known hacking tools. * Targets Windows machines more than MacOS or Linux. * Uses Metasploit and Meterpreter shells to establish persistence and escalate privileges. * Compromises legitimate servers and sites to host their C2 traffic. | Motivations:   * The motivations of the Russian government. * Highly motivated, espionage-focused adversary who aims to obtain diplomatic intelligence. * Targets governments, embassies, military, education, research, and pharmaceutical companies in over 45 countries. | Past Attacks:   * Compromised and overtook the infrastructure of APT34, an Iranian APT, to use for their own work. (2019) * Creates and deploys a RPC backdoor that targets Government systems. (2020) * Deploys a backdoor written in the Microsoft .NET framework that targets government entities. (2017) |