Cozy Bear



|  |
| --- |
| Buff:  +1 SOPH (INT) | +2 TTC (CON) |

|  |  |  |
| --- | --- | --- |
| Techniques:   * Spear-phishing campaigns to deliver malware. * Employs a wide variety of malware types to bring to pass the needs of the Russian gov. * Particularly furtive and stealthy, due to their interest in long-term espionage opportunities. * Low-visibility, difficult to uproot methodology. | Motivations:   * The motivations of the Russian government. * Especially interested in exfiltrating data in such a way that they can keep their foothold and return at a later time. * Oil and Gas, infrastructure, industrials, NGOs, Media, Technology, Government secrets, etc. | Past Attacks:   * Spear Phishing the Pentagon email system (Aug 2015). * Democratic National Committee cyber-attacks surrounding 2016 elections. * SUNBURST supply chain attack on SolarWinds which affected most of the fortune 500 companies through their use of SolarWinds’ third-party services. (Dec 2020). |