The Equation Group



|  |
| --- |
| Buff:  +1 RES (WIS) | +1 SOPH (INT) | +1 DEADL (STREN) |

|  |  |  |
| --- | --- | --- |
| Techniques:   * Use zero-day exploits. * Overwrite the firmware of hard disk drives. * Finds and uses environmental context before deploying payloads. * Heavily uses encryption algorithms and obfuscation techniques. | Motivations:   * Motivations of the U.S. government. * Interested in diplomatic and military intelligence and projects of other countries. | Past Attacks:   * Unconfirmed authors of the StuxNet virus, which damaged nuclear production systems in Iran. * GRAYFISH malware provides an invisible persistence mechanism that allows RCE and complete system access. * Developed the EternalBlue exploit. |