| **Category** | **Description** |
| --- | --- |
| Description | General mid-tiered threat that uses common offensive tools and techniques. |
| Goal and Intent | Exist in the network to enumerate systems and information in order to maintain Command and Control to support future attacks. |
| Key IOCs | PowerShell Empire HTTP agent on TCP 80, Location: Memory Resident and PowerShell Script stored in Registry, HTTP matching HAVEX |
| C2 Overview | HTTPS on port 80 with a 5 second callback. Calling directly to threat-owned domains. |
| TTPs (Enumeration, Delivery, Lateral Movement, Privilege Escalation, etc.) | Initially delivered during exploitation. POST exploitation delivery via PowerShell commands. Enumeration and lateral movement via PS Empire and native Windows commands. Privilege escalation limited and determined POST exploitation. |
| Exploitation | Social Engineering via Phishing, watering hole, and supply chain via compromised web servers |
| Persistence | Persistence via registry RUN key modification |

**THREAT PROFILE EXAMPLE**[**​**](https://redteam.guide/docs/Exercises/threat-profile#threat-profile-example-1)