|  |  |  |
| --- | --- | --- |
| Machines | Summary | Overview, Process List, Network Connections, Services, Software List |
|  | Browser Artifacts | IE, Chrome, Firefox |
|  | Persistence | Startup programs, Registry entries, Scheduled Tasks |
|  | Evidence of Execution | Prefetch, Shim Cache, Lnk Files, Jump List, Open MRU |
|  | Lateral Movement | Remote Desktop Connections, Run MRU |
|  | Gather Evidence | Query, Results |
| Evidence Lookup | Ip |  |
|  | File Hash |  |
|  | Registry |  |
|  | Process Name |  |
|  | Yara Signature |  |