Changes

2.3.0 [2023/12/23] - SECCON Christmas Release

New Features:

- Added the `ttp-visualize` command to extract TTPs and create a JSON file to visualize in ATT&CK Navigator. (#76) (@fukusuket)
- Added the `ttp-summary` command to summarize tactics and techniques found in each computer. (#78) (@fukusuket)

Bug Fixes:

- Fixed a display error (mojibake) in the `timeline-partition-diagnostic` command. (#74) (@fukusuket)

2.2.0 [2023/12/03] - Nasi Lemak Release

New Features:

- Added `timeline-partition-diagnostic` command to parse the Windows 10 `Microsoft-Windows-Partition%4Diagnostic.evtx` log file and report information about all the connected devices and their Volume Serial Numbers, both currently present on the device and previously existed. (Based on https://github.com/theAtropos4n6/Partition-4DiagnosticParser) (#70) (@fukusuket)

Enhancements:

- Improved the display of the progress bar in the `vt-lookup` command. (#68) (@fukusuket)

Bug Fixes:

- Fixed an unhandled exception bug when key is not found. (#65) (@fukusuket)
- Newline handling was not done properly in `extract-scriptblocks` command for JSON input. (#71) (@fukusuket)

2.1.0 [2023/10/31] - Halloween Release

New Features:

- New `extract-scriptblocks` command to reassemble PowerShell EID 4104 ScriptBlock logs. (#47) (@fukusuket)

Enhancements:

- Takajo now compiles with Nim 2.0.0. (#31) (@fukusuket)
- Replaced HTTP with Puppy to reduce external dependencies. (#33) (@fukusuket)
- Made VirusTotal lookups multi-threaded to increase performance. (#33) (@fukusuket)
- Added file existence checks when specifying the timeline. (@fukusuket)
- Added a warning when the timeline is not in JSONL format. (#43) (@fukusuket)
- Output root process information in the `sysmon-process-tree` command. Processes are now sorted by timestamp. (#54) (@fukusuket)

*Bug Fixes:**

- `timeline-suspicious-processes` would crash when Hayabusa results from version 2.8.0+ was used. (#35) (@fukusuket)
- Fixed a JSON parsing error in VirusTotal lookups when an invalid API key was specified. (@fukusuket)
- Fixed a bug in `sysmon-process-tree` in which process information would sometimes be outputted twice. (#52) (@fukusuket)
- `timeline-suspicious-processes` was not correctly outputting `ParentPGUID` field. Improved PID decimal conversion. (#50) (@fukusuket)
- Fixed an error when the specified `PGUID` was invalid or does not exist in the JSONL timeline. (#53) (@fukusuket)

2.0.0 [2022/08/03] - SANS DFIR Summit 2023 Release

New Features:

- `list-domains` : create a list of unique domains. (@YamatoSecurity)
- `list-hashes` : create a list of process hashes to be used with vt-hash-lookup. (@YamatoSecurity)
- `list-ip-addresses` : create a list of unique target and/or source IP addresses. (@YamatoSecurity)
- `split-csv-timeline` : split up a large CSV file into smaller ones based on the computer name. (@YamatoSecurity)
- `split-json-timeline` : split up a large JSONL timeline into smaller ones based on the computer name. (@fukusuket)
- `stack-logons` : stack logons by target user, target computer, source IP address and source computer. (@YamatoSecurity)
- `sysmon-process-tree` : output the process tree of a certain process. (@hitenkoku)
- `timeline-logon` : create a CSV timeline of logon events. (@YamatoSecurity)
- `timeline-suspicious-processes` : create a CSV timeline of suspicious processes. (@YamatoSecurity)
- `vt-domain-lookup` : look up a list of domains on VirusTotal. (@YamatoSecurity)
- `vt-hash-lookup` : look up a list of hashes on VirusTotal. (@YamatoSecurity)
- `vt-ip-lookup` : look up a list of IP addresses on VirusTotal. (@YamatoSecurity)

v1.0.0 [2022/10/28] - Code Blue 2022 Bluebox Release

New Features:

- `list-undetected-evtx-files` : List up all of the `.evtx` files that Hayabusa didn't have a detection rule for. (#4) (@hitenkoku)
- `list-unused-rules` : List up all of the `.yml` detection rules that were not used. (#4) (@hitenkoku)
- Added Logo. If you want to hide the logo, use the `-q, --quiet` option. (#12) (@YamatoSecurity @hitenkoku)
- Added result output option. (`-o, --output`) (#11) (@hitenkoku)