HXTool 4.5

Release notes

FireEye, Inc. I 601 McCarthy Blvd. Milpitas, CA 95035 I 408.321.6300 I 877.FIREEYE (347.3393) I info@fireeye.com I www.fireeye.com

HXTOOL 4.5.0 RELEASE NOTES

NEW FEATURES

- User interface rewritten to accommodate a better user experience
- New chart library enables better interaction with charts
- User interface is now fully API driven to allow a more seamless experience without page reloading
- Agent dashboard, allows users to monitor their agent estates
- All tables should now be exportable to clipboard, excel and csv
- New task-module to allow acquisition upload to FireEye Helix
- Ability to remove alerts
- Ability to remove hosts
- New host drill-down view that provides
    - Hostname, domain, OS, containment state, stateagent status, last poll, Primary IP, agent version, drives, install date, build number, logged on users, isVirtual
    - Full host info and sysinfo
    - Full agent configuration
    - Ability to remove alerts and acquisitions
    - Acquire a file from an alert
    - Pivot to VT, FireEye threat intel, Google
    - See bulk acquisition details on the host-drill-down page
- Two new command line arguments added --clear-sessions and --clear-saved-tasks

BUGFIXES

- Lots of user interface bugs have been deal with as part of the re-write of the interface
- Scheduler has been optimized
- A locking issue was solved in scheduler when writing files to the same directory
- Dockerfile was improved
- API backend logins moved to scheduler so unresponsive controllers do not affect HXTool startup time
- Unified logging code
- Added configuration documentation
- Hundreds of additional minor fixes

KNOWN LIMITATIONS

- Some features greatly depend on the number of alerts/acquisitions or other type of data contained in your FireEye endpoint controller. We have limited means of testing with very large configurations so certain panels or tables might take a while to load. The reason behind this is that we need to poll certain data from the endpoint API which depends on resources, hardware specification where you run HXTool and network performance.
- Data stacking does currently not have any limitations of the number of rows that can be returned. Very large data stacking jobs can potentially return too much data causing long load times and high memory use in your web browser
- Scheduler is multi-threaded and the number of threads can be controlled in the configuration file. When using the feature bulk acquisition with task-processor profiles each thread can allocate up to 800Mb of memory usage. Make sure you have enough memory in your system to accommodate each thread.

With the addition of task processors HXTool can now potentially use much more system resources than earlier versions due to the fact that we are ingesting and processing each acquisition result. If this feature is heavily used, we recommend running HXTool on a dedicated server

FireEye, Inc. I 601 McCarthy Blvd. Milpitas, CA 95035 I 408.321.6300 I 877.FIREEYE (347.3393) I info@fireeye.com I www.fireeye.com