FIREEYE TECHNICAL DOCUMENTATION

HXTOOL 3.0

RELEASE NOTES

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

HXTOOL 3.0 – RELEASE NOTES

NEW FEATURES

- New database backend – TinyDB
- Python 2.7 and 3.x support
- New login page and profile manager
    - Login page will automatically focus to the username field
    - Login page directs to the page you were on when logged out due to inactivity
- Threaded background processor to allow faster data processing of bulk downloads or post-download handlers such as multi-file-acquisition and data-stacking.
- Dashboard now defaults to “today” to limit loading times on controllers with a lot of alerts
- Alert investigation panel introduced. Clicking a host-name or clicking “details” on an alert brings you into this view where you can analyze alerts for that endpoint and also access all acquisitions on one page
    - Alert investigation panel adds “Analysis details” for EXG alerts which is a table that shows the source artifacts causing EXG to block/alert
    - Alert investigation panel displays previously hidden information such as logged in users, last poll ip, last poll timestamp, initial provision timestamp
- Containment, triage, single file acquisition and data acquisition based on custom script added for endpoints
- Find a host search capability to search for a specific hostname with direct access to containment, acquisitions and triage
- Bulk acquisition downloader now uses threaded backend for greater performance
- New Python HX library based on a class and leveraging requests over URLlib2 for greater performance
- Multi-file acquisition feature allowing file-listings across many endpoints with click-to-select user interface to acquire multiple files in one go.
- Re-engineered Data Stacking capability with new stacking options. The new capability leverages new background processor and the new database backend TinyDB
    - All stacking options: Services, Scheduled tasks, Process, Ports, Driver modules, Driver signature, Master boot record and Ports (Linux)
- Real-time indicator export now indents JSON data making it easier to modify before import Platform support for indicators
- Custom configuration channel support (view, add, list)
- Encrypted background processor credentials
- New logging and syslog logging support
- Header and cookie support for HX API communication allowing proxies to be used between
- HXTool and HX Controller

BUGFIXES

Too many to list, HXTool has been reengineered in 3.0 which solved a large quantity of potential problems.

KNOWN LIMITATIONS

- Since the database backend has been changed previous version of HXTool is not compatible with HXTool 3.0 so you have to “start-from scratch” which means you lose your current profiles, event annotations and stacking results.
- When including MacOS or Linux endpoints into a host-set used for data stacking the background processor will fail to process the results
- When importing an IOC which is a member of a non-existing category the code will fail. Create a category with the same name to get around this issue
- Alert investigation panel can take a long time to load on an endpoint with many alerts. This is due to the time is takes to retrieve the alerts via the API and depends on network performance between HXTool and the HX Controller
- If you have thousands of alerts generated “today” the dashboard may take some time to load due to the number of alerts that are being retrived from the HX Controller. You can use HX identical alerts throttling to avoid getting a lot of identical alerts (introduced in HX 4.0.1)
- HX by default logs you out of the API after a short time of inactivity. This configuration can be changed in the HX CLI allowing longer sessions of inactivity in HXTool
- 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