

Assassin v1.3 Commands

run_mode Code specifying the run mode, represented by combining the following keys:
 ' r ' - run the task on receipt
 ' s ' - run the task on every Implant startup
 ' p ' - push the task results to the LP immediately

1 File System Tasks

get <run_mode><r_file> [offset=0] [bytes=0]

Get a file from the target.

put <run_mode><l_file><r_file> [mode='always']

Put a local file on the target.

file_walk <run_mode><r_dir><wildcard><depth> [time_check='no_check'] [date]

Walk the directories on the target, collecting information on files specified by the provided parameters.

get_walk <run_mode><r_dir><wildcard><depth> [time_check='no_check'] [date] [offset=0] [bytes=0]

Walk the directories on the target, collecting files specified by the provided parameters.

delete_file <run_mode><r_file>

Delete a file from the target.

delete_secure <run_mode><r_file>

Securely delete a file from the target. The file is overwritten with zeroes before being deleted.

2 Program Execution Tasks

`execute_bg <run_mode><r_file> [args='']`

Execute a program on the target in the background. The implant will continue to operate. The standard output and return code of the program are ignored.

`execute_fg <run_mode><r_file> [args='']`

Execute a program on the target in the foreground. The Implant will wait for the program to exit. The standard output and return code of the program are captured and returned.

3 DLL Memory Load

`load_faf_bg <run_mode><dll_file_path > [args='']`

Load the provided Fire and Forget V2. DLL into memory and based on its return value, either clear it from memory or leave it running

`load_ice_bg <run_mode><dll_file_path > [args=''] [feature_set='']`

Load the provided ICE V3 DLL into memory, and run it using the provided feature set. If the DLL only supports one feature set, that option will be used and the "feature_set" parameter is not required

4 Configuration Tasks

Configuration Set

`persist_settings <run_mode>`

Save the current settings as the default configuration that will be loaded at Implant startup. Configuration changes must be explicitly persisted, or they will revert on next startup.

`restore_defaults <run_mode><options>`

Restore the Implant configuration to factory settings. Any changes must be persisted explicitly.

Beacon Configuration

`set_beacon_params <run_mode>[initial=0] [default_int=0] [max_int=0] [factor=0.0] [jitter=0]`

Set one or more of the beacon parameters. Note that 0 indicates 'do not alter this value'.

`set_blacklist <run_mode> [programs=[]] [files=[]]`

Set the process blacklist.

`set_whitelist <run_mode> [programs=[]] [files=[]]`

Set the process whitelist.

Comms Configuration

`set_transport <run_mode> [xml_file=None]`

Set the communication transport configuration.

`set_chunk_size <run_mode><chunk_size>`

Set chunk size to limit network traffic per beacon.

Operation Window Configuration

`set_hibernate <run_mode><seconds>`

Set the hibernate time in seconds after first execution. The Implant will lie dormant until the hibernate period has elapsed.

`set_uninstall_date <run_mode><date>`

Set the uninstall date for the implant.

`set_uninstall_timer <run_mode><seconds>`

Set the uninstall timer to seconds from time the task is processed by the Implant.

`set_beacon_failure <run_mode><count>`

Set the maximum number of sequential beacon failures before uninstalling.

Safety

`safety <run_mode><seconds>`

Set the Implant beacon interval during idle beacons. This task will not generate a result.

`set_interval <run_mode><seconds>`

Set the Implant beacon interval. This task will not generate a result. This command is used by the 'safety' command and is required by Collide. It is not recommended for use by operators; see the `set_beacon_params` task.

5 Maintenance Tasks

`get_status <run_mode><status_mode><options>`

Request the current Implant configuration and status information.

`clear_queue <run_mode>`

Clear all files from the Implant upload queue. The `clear_queue` task will delete all files from the output, push, and staging directories on target. This may include chunks of files that have been partially uploaded.

`upload_all <run_mode>`

Upload all files currently in the upload queue. The `upload_all` task will upload all files in the output, push, and staging directories to the listening post as quickly as possible, ignoring the chunk size setting.

Warning: This is a dangerous task and may have adverse effects if the upload queue has a significant backlog. Please use the `get_status` command with the `dir_files` option to decide if the risk is acceptable.

`unpersist <run_mode>`

Stop the Implant persistence mechanism on the target.

`uninstall <run_mode>`

Uninstall the Implant from the target immediately.

