IR Distill

IR Distill essentially reduces the amount of lines an analyst has to review from Amcache/RecentFileCache/Shimcache tool output. It is primarily used during mass triage for frequency analysis. For example, the SHA1 hashes from the Amcache(s) can be compared to the hashes listed in the NSRL database and multiple white/review lists. The matching hashes to the databases can be ignored, and the unknown can be reviewed.

Besides SHA1 hashes for filtering, full path and filenames can be used for filtering. While it is not a 100% in identification of benign binaries, it does help to highlight the unknown filenames found within the Amcache/RecentFileCache/Shimcache tool output. The tool compares the fullpath and filename against the filecheck and reviewlist databases. Unfortunately, the NSRL database does not include the full path for where the binaries are found. Due to that, RecentFileCache and Shimcache can only be examined with the --filecheck and --reviewlist options.

Command Line Options

Short hand Argument	**Long Hand Argument**	**Description**
-n	--nsrl	Check SHA1 hashes against NSRL SQLite database
-f	--filecheck	Check file name & full path against OS Distill SQLite database
-i	--infile	Either the frequency analysis containing file name & full path or file contains SHA1 hashes from amcache
-o	--out	Output file name
	--showallmatches	Show all matches from –filecheck
	--ignorecase	Ignore case in file name and full path during –filecheck
-r	--reviewlist	Review list/White list SQLite database(s); May provide single files and/or directory containing the databases

Steps for Reviewing AppCache/ShimCache

1) Gather the system hives
2) Use RegRipper and use the modded appcompatcache_tln (https://github.com/chaoticmachinery/mass_triage_tools/tree/master/regripper_plugins) to process the hives
3) Create freq. analysis file per my sans article
4) ./ir_distil_v0.3.py --filecheck os.sqlite -i appcache_freq -o outfile1 --ignorecase --reviewlist /data/whitelist/filelist.db
5) Review “nomatch” file from output

Steps for Reviewing Amcache

1) Gather the amcache hives
2) Use RegRipper and use the modded amcache_tln (https://github.com/chaoticmachinery/mass_triage_tools/tree/master/regripper_plugins) to process the hives

3) Extract SHA1 hashes from output (step2)

   ```
   cut -f8 -d\| amcache{datetime}.txt | sort | uniq | grep -v amcache | sed '/^[[:space:]]*$/d' | grep -v -i "plugins" > amcache{datetime}.sha
   ```

4) Run SHA1 hashes through OS Distill NSRL

   ```
   ./ir_distil_v0.3.py  --nsrl ./nsrl.db -i amcache{datetime}.sha -o outfile0 --ignorecase  --reviewlist /data/whitelist/filelist.db
   ```

5) Review column 6 (Application type) “match” file for general categories. If there is a category that should be not be on the network, grep the category out of the “match” file to find more information.
6) Pull out the SHA1 hashes from the “match” file and pull those lines out of the output file from step 2 and create freq. analysis.

   ```
   grep -a AmCache_ ".$outfilereg." | grep -v Hive: | grep -v -f ".$nsrlsha1." | cut -f7 -d\\| | sort | uniq -c | sed -e 's/^[ \t]*//' | sort -t' ' -k2 > amcache{date}_fq.txt
   ```

7) Run amcache{date}_fq.txt through OS Distill filecheck

   ```
   ./ir_distil_v0.3.py --filecheck os.sqlite -i amcache{date}_fq.txt  -o outfile1 --ignorecase  --reviewlist /data/whitelist/filelist.db
   ```

8) Review outfile1 “nomatch” file for badness