Sample Finder

Joren

Problem

- You read a cool CTI blog
- You want to analyze the samples mentioned in the blog
- How do you find the samples?
  - e.g. if they are not on VirusTotal

Filename	Hash	
libpe.so	MD5	6c0adca790235445d07be98cd0f820b5
	SHA1	cd6944926169f56ba78cdf15df6eea44b267bb51
	SHA256	50451bb5b6d68115695a6cb277839a6dd2bad8f70bdb8b79670b18dcde188965
smartctl	MD5	205a8c6049061930490b2482855babcd
	SHA1	77698f3f915e61852b6a79bbd85744d845b112c4
	SHA256	4519baebba73827e2b33f36f835d6cb704755abf1312d8d197be635f4d9ffade
authd	MD5	9124ce75319514561156d2013fc9d3be
	SHA1	b59d6ec835329ea8982fbbe87bb6b6132514c491
	SHA256	f40c04fb9e2d4157a0bc753925dbc5f757feb77cdd22f90fedf3cc5e095143bc
httpsd	MD5	218a3525ab8e46f7afe252d050a86907
	SHA1	44ed7bf2187c5f7442d8167ef009598dbbed60cb
	SHA256	3ed99aad5922744b6a75ea90ea6ece81ba0d8eb9935aec38b897e44ac3b36c35
	TLSH	T1C7829327B751CA79C099F7B05CAF8AB07836B0F4E722621F2241A6797C647844F0F766
	SSDEEP	192:GTHZecX8f8fUlxblVKmu6Wt9ygq1OtHCj31DM8MC3RUJET+mFG7vSif:kZe18fUl17WlqUtiL1h36iTnYj
newcli	MD5	ab89139e3d47fbaba2da33040da95200
	SHA1	302743eaaa12018647b67b390a270ed98d3219d6
	SHA256	2acc6a2a931db63fe3a875780f00192a60955c9794df68fe0ace0012d309b04f
preload.so	MD5	a62377c01935f366761846b5ceed5a49
	SHA1	c259f0efa8ff0ea798a6a3dda22b8df62627405b
	SHA256	1c437dc9e929669e5a65a1c70afb3107fba471afb9ad35e3848334c9332f2b59

Sample Finder

- Searches multiple (free/public) sources for a list of hashes:
  - Malpedia
  - Malware Bazaar
  - MalShare
  - VirusShare
  - Triage
  - New sources can be added easily

pip install sample-finder

https://github.com/joren485/sample-finder