THOR v10.5 – June 2020

New Feature and Changes

THOR v10.5

- A minor release with the most new features since THOR v10.0
- Result of the March / April / May Development Sprint

PE Sieve Integration

- PE Sieve by @hasherezade
- Process anomaly detection: hooks, process hollowing, process doppelgänging, reflective DLL injection
- Available in THOR Lite

build passing | code quality A | License BSD 2-Clause | release v0.2.6.1 | downloads 64k | Tweet

❓ FAQ - Frequently Asked Questions

📖 Read Wiki

PE-sieve is a tool that helps to detect malware running on the system, as well as to collect the potentially malicious material for further analysis. Recognizes and dumps variety of implants within the scanned process: replaced/injected PEs, shellcodes, hooks, and other in-memory patches.
Detects inline hooks, Process Hollowing, Process Doppelgänging, Reflective DLL Injection, etc.

PE-sieve is meant to be a **light-weight engine** dedicated to scan **a single process** at the time. It can be built as an EXE or as a DLL. The DLL version exposes a simple API and can be easily integrated with other applications.

If instead of scanning a particular process you want to scan your **full system** with PE-sieve, you can use HollowsHunter. It contains PE-sieve (a DLL version), but offers also some additional features and filters on the top of this base.

Uses library: https://github.com/hasherezade/libpeconv.git

YARA 4.01

- Massive memory usage improvements
  - Windows -70%
  - Linux -55%

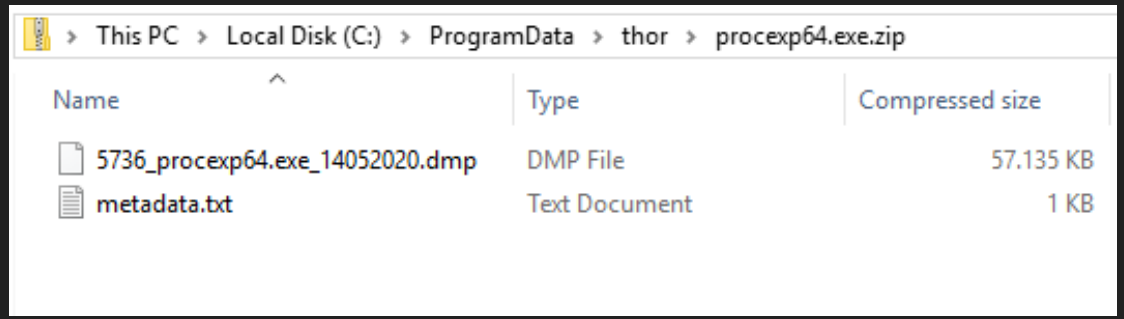
VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
317748	236800	16780	D	3.0	0.7	0:52.29	./thor10.5 --nodoublecheck
620572	540936	16568	D	2.3	1.7	1:27.22	./thor10.4 --nodoublecheck

Process	CPU	Private Bytes	Working Set	PID
thor10.5.exe	2.77	325.144 K	156.616 K	3996
thor10.4.exe	7.17	432.180 K	429.384 K	31648

Process Memory Dumps

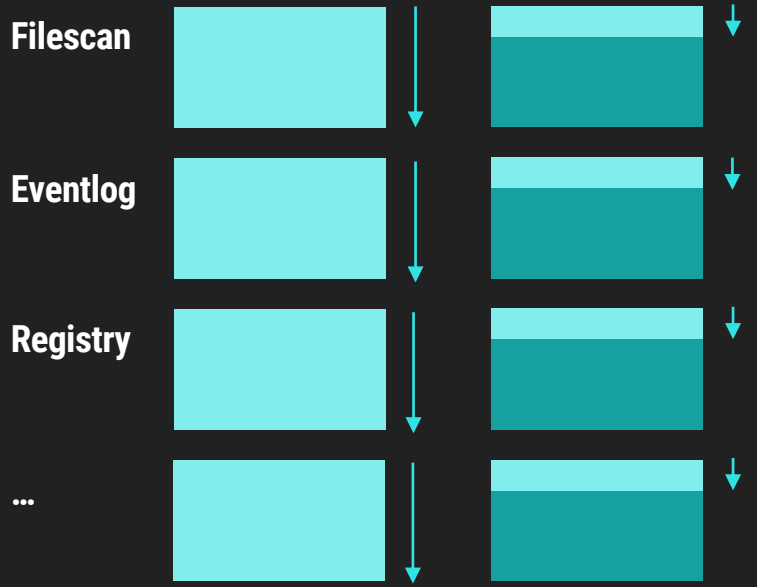
- Matches on process memory create process memory dumps in C:\ProgramData\thor
- Enable: **--dump-procs**
- With metadata.txt
  - Process name, matching YARA rule, offset of matches in memory
- Safe guards
  - New match on same process overwrites old file
  - Available disk space checks

```
Warning: ProcessCheck YARA rule match on process memory RULE: Example_Rule TAGS:  DESC: Example r
ule to match a process SCORE: 75 REFERENCE: not set RULEDATE: 2019-05-14 PID: 5736 NAME: procexp6
4.exe CMD: "C:\Users\Max\Downloads\PROCEXP64.EXE"  USER: DESKTOP-EEM5B52\Max MATCH_STRINGS: Str1:
 "procexp"
Info: ProcessCheck Successfully dumped process PID: 5736 PPID: 3320 PARENT:  NAME: procexp64.exe
OWNER: DESKTOP-EEM5B52\Max COMMAND: "C:\Users\Max\Downloads\PROCEXP64.EXE"  PATH: C:\Users\Max\Do
wnloads\PROCEXP64.EXE
CREATED: Mon May 11 14:27:58 2020
MD5: 7e7eaa8aebc4026be3b56b965b0d8947 CONNECTION_COUNT: 0 LISTEN_PORTS:  FILE_1: C:\Users\Max\Dow
nloads\PROCEXP64.EXE EXISTS_1: yes MD5_1: 7e7eaa8aebc4026be3b56b965b0d8947 SHA1_1: 57fe177df7e94b
a8495e1885c9b5946fa4312df3 SHA256_1: aac11d3ff8661e14a6d7073e44f0d6ccabc436856af5faf10e761c57e8b4
2f71 FIRSTBYTES_1: 4d5a900003000000040000000ffff0000b8000000 DUMP_FILE: C:\ProgramData\thor\procex
p64.exe.zip
Info: ProcessCheck Finished module TOOK: 0 hours 0 mins 9 secs
```



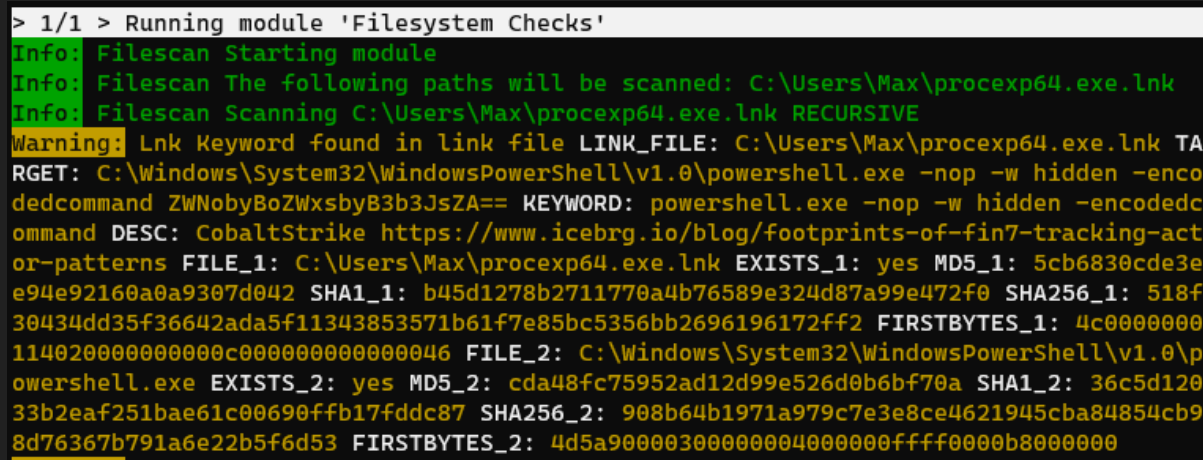
Global Lookback

- Instructs THOR to scan only elements changed or created in the last X days
- New flag **--global-lookback** (used with **--lookback X**)
- Example: **--lookback 3 --global-lookback**
- Massiv reduction of scan duration
- Full scan with global lookback: <30 min
- Best scan mode for Microsoft Defender ATP integration



Link File Parser (LNK)

- Parses contents of Windows link files (.lnk)
- Applies all IOCs and anomaly rules to the linked files and folders
- Message enrichment to get hash values & FIRST_BYTES for each referencd file



Customer Portal Integration

- New --portal* flags
  --portal-contracts [list of ids]
  --portal-key [APIKEY]
  --portal-nonewlic
- Allows to generate a new license at runtime via the API
- Best practice: Set these values in the YAML config (./config/thor.yml)

Customer Portal

Contract ID	Contract Type	Description	Limit	Spent	Left
Search	Worl	Search	Sear	Searc	Sea
13	Workstation	Workstation License Pool (400)	400	1	399
14	Server & Workstation	Server License Pool (400)	400	0	400

thor.yml

```yaml
# This is the default con
# Skip files bigger than
max_file_size: 4500000
buffer_size: 4500000
# Minimum score to report is 40
min: 40
# Terminate THOR if he runs longer than 72 hours
max_runtime: 72
# Limit THOR's CPU usage to 70%
#cpulimit: 70
# The minimum amount of free physical memory to proceed (in MB)
minmem: 50
# Truncate THOR's field values after 750 characters
truncate: 750

portal-contracts:
  - 13
  - 14
portal-key: 34dh78I02Py8dCg9RKKXNRdCCZc27JpQuPxfnPQEQo8
```

More Changes

- Default output files include a timestamp and not just the date
- THOR DBs “**--resume**” feature is deactivated by default and has to be manually activated using “**--resume**” due to significant performance implications caused by updating resume states in THOR DB
- New **--scanid-prefix X** allows users to set a custom prefix to allow the identification of group of scans
- New **--print-signatures** flag lists names and meta data of all included YARA and Sigma rules

Upcoming in July 2020 : THOR GUI

- Simple GUI for THOR and THOR Lite