IME USP kaspersky

AmCache-EvilHunter

Automating Evidence of Execution Extraction from the `Amcache.hve` Artifact

Cristian Souza, Eduardo Ovalle and Daniel Batista

DFIR Specialist, Ph.D Candidate

Agenda

Introduction

- DFIR investigations depend on the ability to quickly identify what was executed, installed, copied, or present on a compromised system.
- This information is important because attackers frequently remove their tools after execution or rename malicious files using legitimate Windows process names.

Introduction

- The `Amcache.hve` artifact stores rich metadata about executables and drivers, including file paths, compilation timestamps, publisher information, file sizes, and **SHA-1 hashes**.
- It may preserve information about files that were deleted, renamed, or otherwise lost during an attack.

Introduction

- This work introduces `AmCache-EvilHunter`, an open-source command-line tool to parse and analyze Windows `Amcache.hve` registry hives.
- The main goal is to reduce manual effort during triage and help analysts quickly identify records that deserve deeper investigation.

Background and related tools

Relevant `Amcache.hve` keys:

- `InventoryApplicationFile`
- `InventoryApplication`
- `InventoryDriverBinary`
- `InventoryApplicationShortcut`

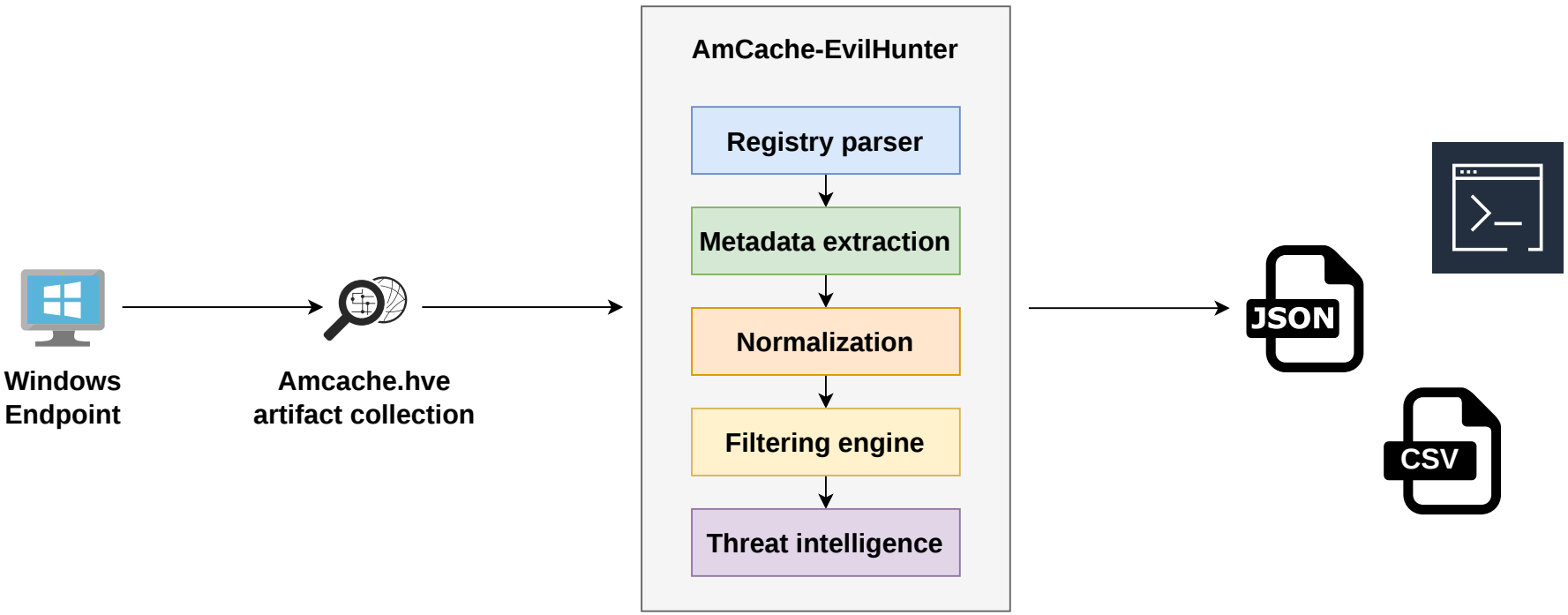
Background and related tools

Table: Comparison between AmCache-EvilHunter and related tools.

Feature	**This work**	**AmcacheParser**	**KAPE**	**Velociraptor**
Parse `Amcache.hve`	✓	✓	✓	✓
CSV export	✓	✓	✓	✓
JSON export	✓	✓	✓	✓
Date filtering	✓	–	–	Limited
Keyword search	✓	–	–	Limited
Suspicious executable detection	✓	–	–	–
Threat intelligence enrichment	✓	–	–	Limited

Architecture and implementation

Figure: General architecture of AmCache-EvilHunter.



Architecture and implementation

- `AmCache-EvilHunter` requires Python 3.7 or higher.
- The user can enable OpenTIP lookups with `--opentip` and VirusTotal lookups with `-v` or `--vt`.
- Lookup results are cached during execution to avoid repeated requests for the same hash.
- The user can choose to export results to CSV or JSON Lines for reporting, timeline analysis, or further processing.

Usage

Figure: Basic usage of AmCache-EvilHunter to parse an `Amcache.hve` file.

```
$ ./AmCache-EvilHunter.py -i Amcache1.hve --csv output.csv
```

SHA-1	Name	RecordDate	OS?
11eba7b1e26cc7d492a2c161ac48370811d0b01e	csrss.exe	2024-09-04T19:25:16.972623	Yes
3d26b0dc519e04999118f4a02ea8acd5f1db8feb	MicrosoftEdgeUpdate.exe	2024-09-04T19:25:16.988337	No
010db07461e45b41c886192df6fd425ba8d42d82	svchost.exe	2024-09-04T19:25:16.988337	Yes
e3e0f810ef3e0a36c13c97eee8246784fb7cbfca	TiWorker.exe	2024-09-04T19:25:17.004080	No
77f2e744c92417653b5abd6ccb3b5e521111979a	CompatTelRunner.exe	2024-09-04T19:25:17.092058	Yes
0646f86530602a6d5980ad9d460e45f77ef46399	DeviceCensus.exe	2024-09-04T19:25:17.092058	Yes
7b2e3990de386df08a049ecb611bc9ab17c1497c	winlogon.exe	2024-09-04T19:26:42.749811	Yes
647ff5972f7b41ceec7572ef051fd8dde39d9993	msedge.exe	2024-09-04T19:26:45.559471	No
ce8669d8826c8795115d58c62e726ae53943dce9	OneDriveSetup.exe	2024-09-04T19:27:08.364932	Yes
5d6102f5a170e982c7735bfc2b9c1a0a0d435fd1	msiexec.exe	2024-09-04T19:28:07.277472	Yes
2de3263c0aac35367b7db9de2b2ca05f20068a52	drvinst.exe	2024-09-04T19:28:07.321125	Yes
2ff161a1185b5716ade6b895127d561299e7cafe	OneDriveSetup.exe	2024-09-04T19:30:08.018908	No
cab6666a502e4c945f95f78d77e60e025f5c592f	ChromeSetup.exe	2024-09-04T19:33:08.934714	No

Usage

Figure: Identification of suspicious artifacts.

```
$ ./AmCache-EvilHunter.py -i Amcache2.hve --find-suspicious
```

SHA-1	Name	RecordDate	OS?
11eba7b1e26cc7d492a2c161ac48370811d0b01e	csrss.exe	2024-09-04T20:04:09.746658	Yes
010db07461e45b41c886192df6fd425ba8d42d82	svchost.exe	2024-09-04T20:04:09.746658	Yes
4db5a8e237937b6d7b435a8506b8584121a7e9e3	svchost.exe	2024-09-04T20:12:49.216136	No
bd59d7c734ca2f9cbaf7f12bc851f7dce94955d4	123.exe	2024-09-04T20:19:22.164874	No

Usage

Figure: Identification of suspicious artifacts.

```
$ ./AmCache-EvilHunter.py -i Amcache2.hve --find-suspicious --missing-publisher --exclude-os
```

SHA-1	Name	RecordDate	OS?
4db5a8e237937b6d7b435a8506b8584121a7e9e3	svchost.exe	2024-09-04T20:12:49.216136	No
bd59d7c734ca2f9cbaf7f12bc851f7dce94955d4	123.exe	2024-09-04T20:19:22.164874	No

Usage

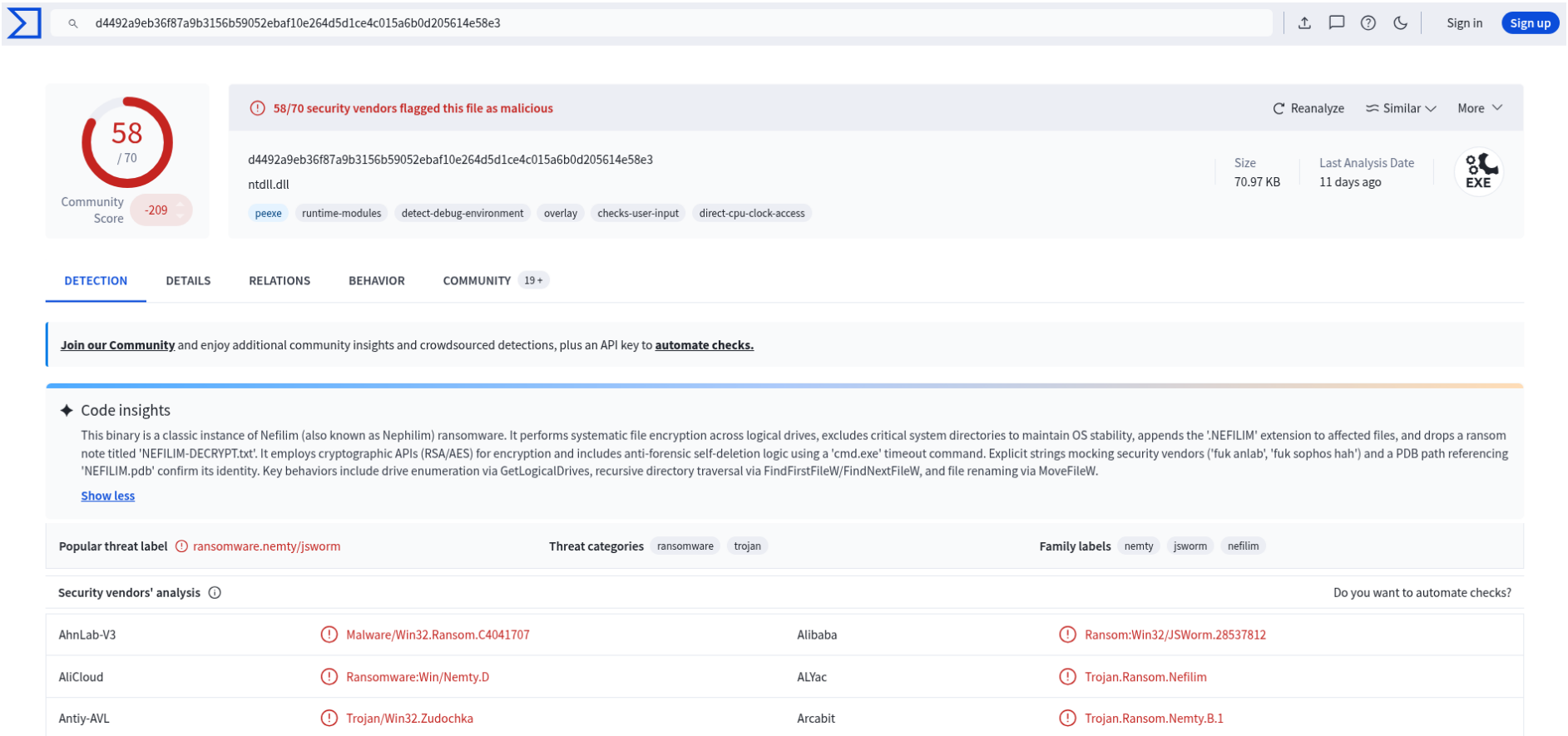
Figure: Threat intelligence lookup using Kaspersky OpenTIP.

```
$ ./AmCache-EvilHunter.py -i Amcache2.hve --find-suspicious --opentip --only-detections
```

SHA-1	Name	RecordDate	OS?	OT
4db5a8e237937b6d7b435a8506b8584121a7e9e3	svchost.exe	2024-09-04T20:12:49.216136	No	Malware
bd59d7c734ca2f9cbaf7f12bc851f7dce94955d4	123.exe	2024-09-04T20:19:22.164874	No	Malware

Usage

Figure: VirusTotal lookup for a suspicious SHA-1.



Conclusion

- This paper presented `AmCache-EvilHunter`, an open-source tool designed to support Amcache-based triage during DFIR investigations.
- The tool parses `Amcache.hve` registry hives and applies multiple filters according to the analyst's needs.
- It also exports results to CSV and JSON, and integrates Kaspersky OpenTIP and VirusTotal lookups.
- Useful in DFIR cases involving deleted malware, renamed binaries, and suspicious drivers or executables.

IME USP kaspersky

AmCache-EvilHunter

Automating Evidence of Execution Extraction from the `Amcache.hve` Artifact

Cristian Souza, Eduardo Ovalle and Daniel Batista

DFIR Specialist, Ph.D Candidate