Detecting and Analyzing Malicious Artifacts for Timely Protection

- Specialized data structures $\cup$ Similarity Digest algorithms = Apotheosis, an approximate SD nearest neighbors system [1]
- Extensible architecture design for multipurpose usage
- Two query searches: K-NN or similarity threshold
- Allow-list dataset of Windows system processes
- REST API interface (Software-as-a-Service model)

**Apotheosis Data Structures**

- **Radix Tree** [2]
  - Insert complexity: $O(m - A)$
  - Search complexity: $O(m)$
  (m: length of the string and A: size of the alphabet)

- **HNSW** [3]
  - Insertion and search complexity: $O(N \cdot \log N)$

**Evaluation**

INSERT results for $M=32$, $ef=4$, $N=10000$

EXACT SEARCH results for $M=32$, $ef=4$, $N=10000$

AKNN SEARCH results for $M=32$, $ef=4$, $N=10000$

**Conclusions**

- **Apotheosis** is an extensible, versatile system that leverages approximate search methods for similarity digests
- Database of Windows OS modules built as an allow-list
- REST API interface available for Apotheosis with our database
  (free access allowed for CERTs and research centers, contact us)

**References**


**Contact data:** reverseame@unizar.es

**Acknowledgements**

- Spanish Ministry of Science and Innovation under grant TEC2021-131115A-I00 (MMIFA); Spanish National Cybersecurity Institute (INDECI) under the Recovery, Transformation and Resilience Plan funds, financed by the European Union (Next Generation); and University, Industry and Innovations Department of the Aragonese Government under Programa de Proyectos Estratégicos de Grupos de Investigación (DeCo research group, ref. TCI-23R; SD research group, ref. T42-23R).

**Use Cases**

- Windows system module similarity digests
- $> 13K$ Windows system processes dumped
- $\approx 2.7M$ of similarity digests (at page-size granularity)
- Different versions of Microsoft Windows operating system
- Similarity digest algorithms: TLSH, SSDEEP, SDRASH

**Allow-List Dataset**

- Windows system module similarity digests
- REST API interface available for Apotheosis

**Scanning QR Code**

Scan the QR to see the code on GitHub!
(under GNU/GPLv3 license)