CRII: SaTC: Towards Paving the Way for Large-Scale Malware Analysis: New Directions in Generic Binary Unpacking

Over the past two decades, packed malware is always a veritable challenge to anti-malware solutions!

UNIVERSITY OF TEXAS ARLINGTON

Challenge:

- Binary packing recovers the original code at run time.
- 80% malware samples are unpacked to evade detection.
- Existing unpacking methods' limitations: 1) high runtime overhead; 2) lack of anti-analysis resistance.

Solution:

- Efficiently determine the end of malware unpacking using a new, reliable feature (**BinUnpack, CCS'18**).
- Completely reconstruct import address table via API micro execution and hardware-assisted control flow monitoring.
- Accurately locate original entry point via symbolic execution and machine learning techniques.

NSF CNS #1850434,
University of Texas at Arlington ,
Computer Science and Engineering Department,
Jiang Ming

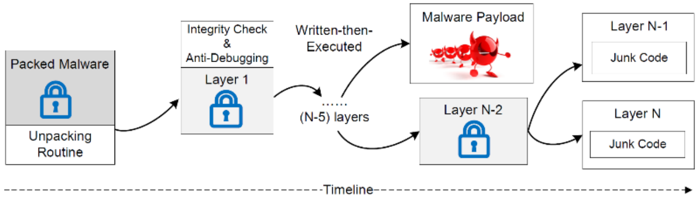
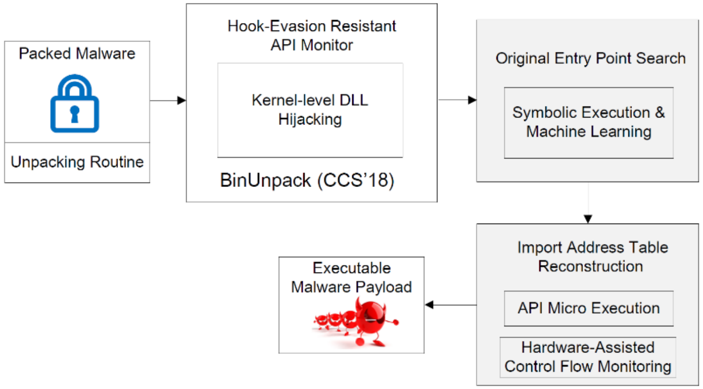


Figure 1: The unpacking process goes through multiple "written-then-executed" layers. The first layer contains anti-analysis code such as integrity check and anti-debugging, and the deepest layer does not consist of the malware payload but junk code.



Packed Malware
Unpacking Routine
Hook-Evasion Resistant API Monitor
Kernel-level DLL Hijacking
BinUnpack (CCS'18)
Original Entry Point Search
Symbolic Execution & Machine Learning
Import Address Table Reconstruction
API Micro Execution
Hardware-Assisted Control Flow Monitoring
Executable Malware Payload

Figure 2: Our research aims to first achieve the ultimate goal of malware unpacking: deliver an executable version of original malware. Our new research tasks are the modules in grey.

Scientific Impact:

- Develop a generic binary unpacking solution with orders-of-magnitude performance boost.
- Pave the way for large-scale malware analysis
- Advance the research community's knowledge on the cyber arms race.

Broader Impact:

- Help security experts respond to emerging malware attacks promptly.
- **BinUnpack** has been deployed into production environment.
- Develop binary unpacking labs to enhance UTA security courses.
- McNair scholar and GAANN fellowship students are participating in the project.