IMPROVING DETECTION AND PROTECTION AGAINST ANTI-SANDBOX TECHNIQUES

BRNO UNIVERSITY OF TECHNOLOGY — FACULTY OF INFORMATION TECHNOLOGY

Excel@FIT 2026

Author: Bc. Jakub Kratochvíl 2026

0x0 Introduction

- Modern malware actively **detects** when it is running in a sandbox and suppresses its behavior to **avoid** analysis.
- This work contributes to **four primary areas** to improve Gen Digital's malware analysis pipeline.

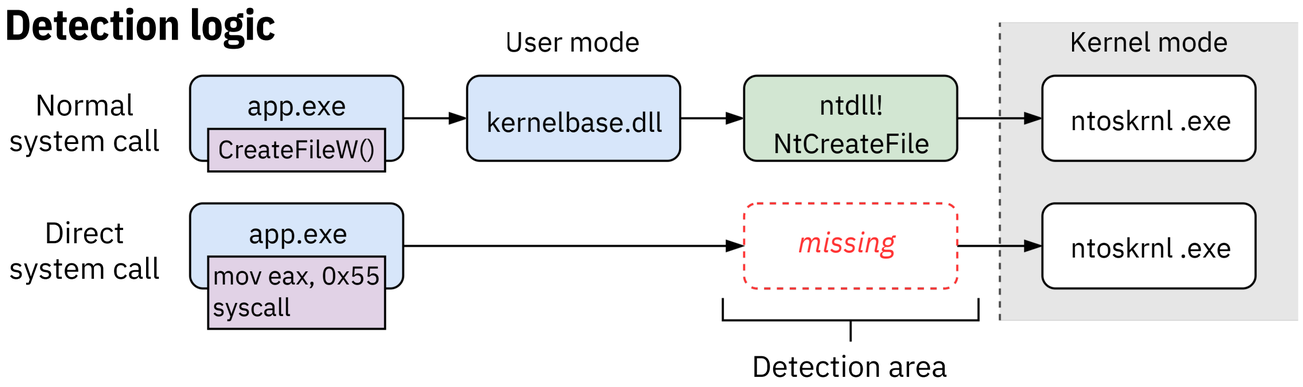
0x1 Areas of Improvement

1. **Signature coverage:** Low detection signature coverage for anti-sandbox techniques in CAPEv2.
2. **Firmware Hardening:** Gaps in virtual machine hardening that leave virtualization indicators exposed in firmware tables.
3. **Evasive Exits:** Absence of a post-analysis mechanism for detecting evasive exits following anti-sandbox checks.
4. **Direct Syscalls:** An architectural gap by which direct system calls bypass CAPEv2's user-mode analysis entirely.

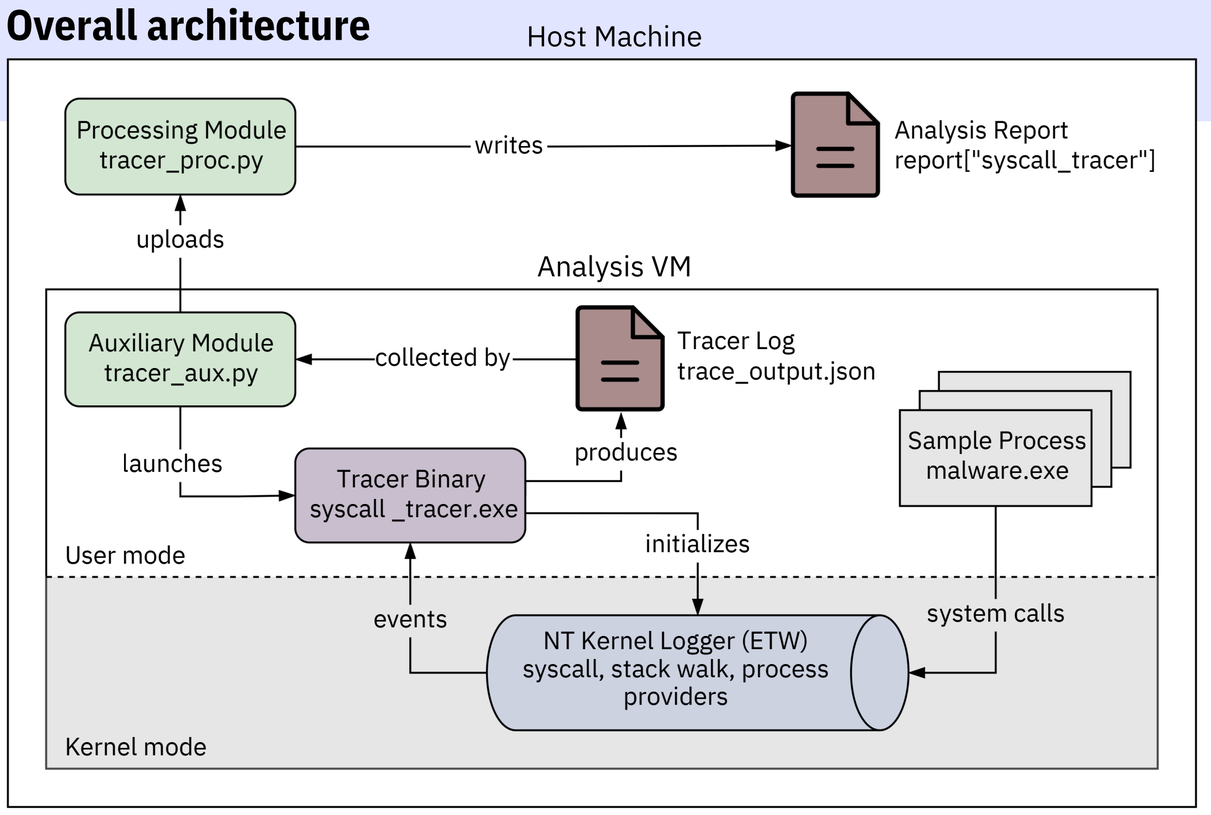
0x2 Direct System Call Tracer using Event Tracing for Windows

- Fully **automated** within CAPEv2 — deployed per analysis, with logs returned to the host and parsed into analysis results.
- ETW streams events to a user-mode consumer, giving syscall visibility **without a kernel driver** and with negligible overhead.

Detection logic



Overall architecture



0x3 Firmware Table Hardening in SeaBIOS

- Targets **Legacy BIOS**, **SMBIOS**, and **ACPI** tables at SeaBIOS to remove QEMU-generated virtualization indicators.
- Handles leftover BIOS strings and **XOR-obfuscates** unmodifiable values (e.g., CPUID signatures).

BEFORE (unpatched)

```
0x0000  52 53 44 54 34 00 00 00 01 62    RSDT4....b
0x0010  42 4F 43 48 53 20 42 58 50 43    BOCHS BXPC
0x0020  20 20 20 20 01 00 00 00 42 58        ....BX
0x0030  50 43 01 00 00 00 BC 28 FE 7F    PC.....(
0x0040  B0 29 FE 7F 40 2A FE 7F 7C 2A    .)  @*   *
```

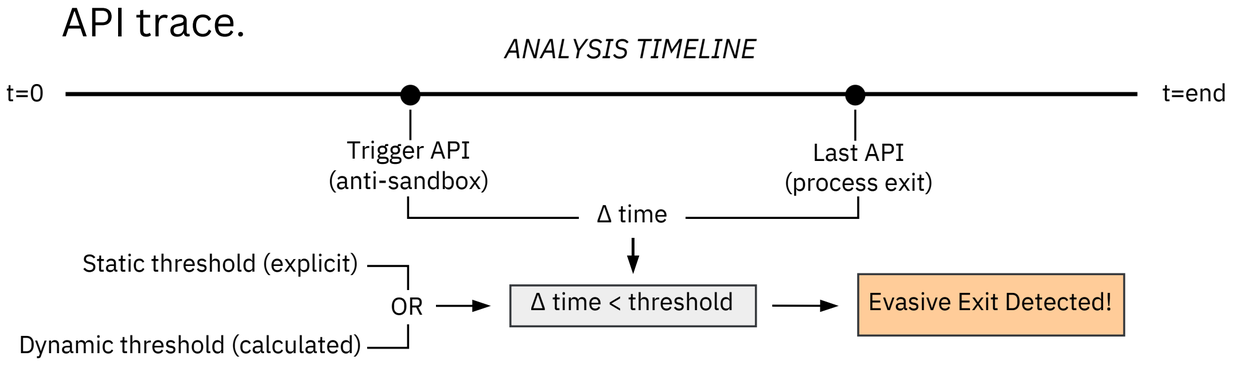
↓

AFTER (patched)

```
0x0000  52 53 44 54 30 00 00 00 01 DF    RSDT0.....
0x0010  41 4C 41 53 4B 41 41 20 4D 20    ALASKAA M
0x0020  49 20 20 20 09 20 07 01 41 4D    I    .   AM
0x0030  49 20 13 00 01 00 57 1F FE 7F    I ....W
0x0040  4B 20 FE 7F DB 20 FE 7F 00 00    K     ....
```

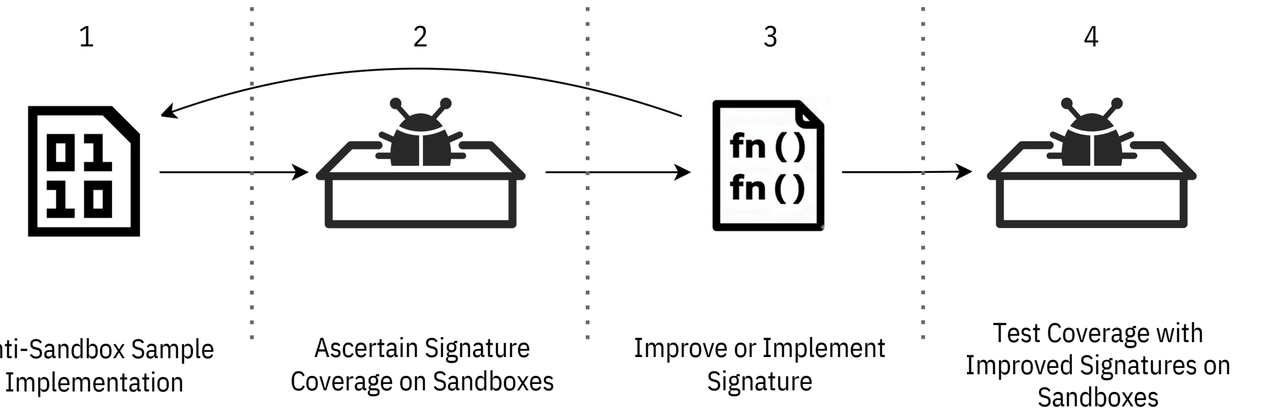
0x4 Post-Analysis Evasive Exit Detection Module

- Runs during CAPE's signature evaluation, reusing the **existing** API trace.



0x5 Anti-Sandbox Simulation Samples & CAPEv2 Signatures

- **82** samples in **30** techniques and **40** implemented signatures.



In partnership with Gen™