BluePill: Neutralizing Anti-Analysis Behavior in Malware Dissection

Daniele Cono D'Elia


WHAT IF THEY FIND OUT
I MISSED ALL THE
MOVIES?

WHO AM I

- Post-doc @ Sapienza University of Rome
- Background in programming languages, using it for software security problems
- Currently: malware, code obfuscation, code reuse techniques

@dcdelia

MALWARE EVASION

- Upsurge of adversarial techniques for dynamic analysis
- New designs for transparent sandboxes: say, Virtual Machine Introspection. What about manual **dissection** though?

Analysts

- love their good old tools and VMs
- want to monitor and alter behaviors
- happy to dodge semantic gaps

IN THIS TALK

- What we did
- Methodology
- Using BluePill

WHAT WE DID

An active approach to transparency: fix artifacts while analysts work.

(WE NEED TO NEUTRALIZE RED PILLS FOR EVASION)

ANALYSTS CONTINUE DISSECTING THE SAMPLE

ANALYSTS FORCED TO START OVER

DESIGNED AROUND ANALYSTS

Coordinated fake answers to meet a sample's expectations

New dissection capabilities

- stealth live patching
- cloaking analysis tools
- user-supplied hooks

Users adjust/write hooks to deal with new patterns

THE NATURE OF EVASIONS

Lessons we learned from literature

- many angles to cover!
- expect coordinated queries with different primitives
- evasions may be general or for specific systems
- slow reaction to new evasions

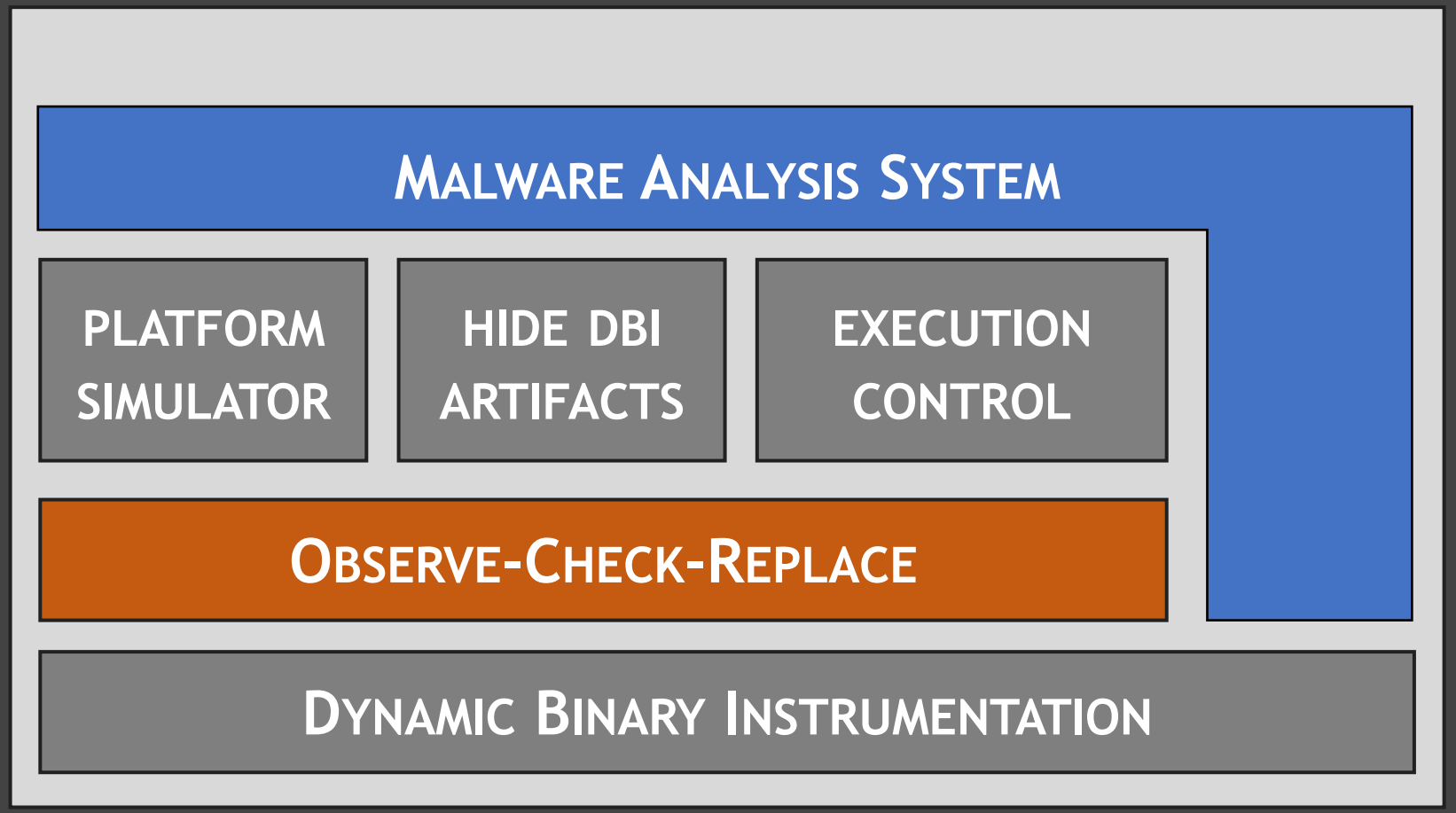
IN THIS TALK

- What we did
- Methodology
- Using BluePill

METHODOLOGY

PARADIGM

- OBSERVE
- CHECK
- REPLACE



DYNAMIC BINARY INSTRUMENTATION

Why this technology

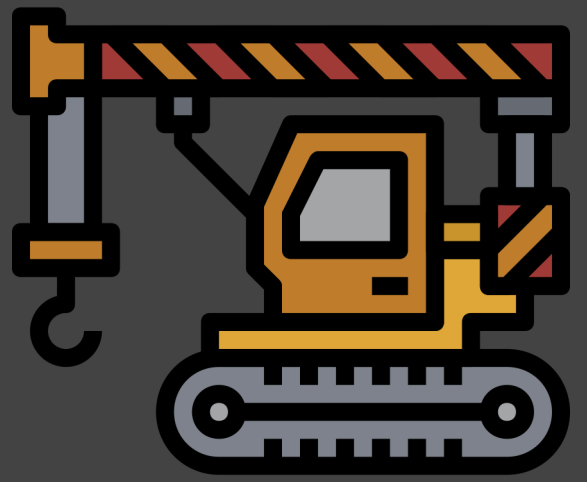
- ✓ easy to encode extensions
- ✓ no semantic gaps
- ✓ per-process faking is easier
- ✓ analysis code not visible to sample
- ✗ but confined to user space

PLACING PROBES

HOOKS

- special instructions
- library calls
- syscalls
- WMI subsystem
- exceptions

Analysts can easily add/tweak hooks...



TIME BEHAVIOR

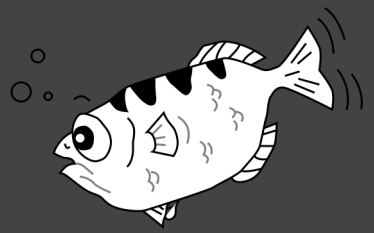
INTUITION

- two enemies: overhead detection, time stalling
- patching time primitives independently won’t work
- fast forward sleeps but accumulate required quantities Q
- for any time query return Q + some Δ

Why?

- hardly sound, but can work in practice
- accelerating one process less likely causes system instabilities

EXECUTION CONTROL



GDB REMOTE INTERFACE

[...]

HOOKS FOR ARTIFACTS

[...]

STEALTH CODE PATCHING

- replace with trampoline to ad-hoc region: arbitrary patch length
- DBI abstraction hides code edits: program reads original bytes

DBI EVASIONS

We build on state-of-the-art mitigations for DBI artifacts

SoK: Using Dynamic Binary Instrumentation for Security (And How You May Get Caught Red Handed) – ACM ASIACCS 2019

https://github.com/season-lab/sok-dbi-security/

ADDITIONS IN BLUEPILL

- hide DBI overheads
- counter new artifacts from DBI debugging

PROGRAM ANALYSES

Value in reverse engineering

- powerful (e.g. symbolic execution, taint analysis)
- but... slowdown/scalability 😭
- using them blindly may just not work

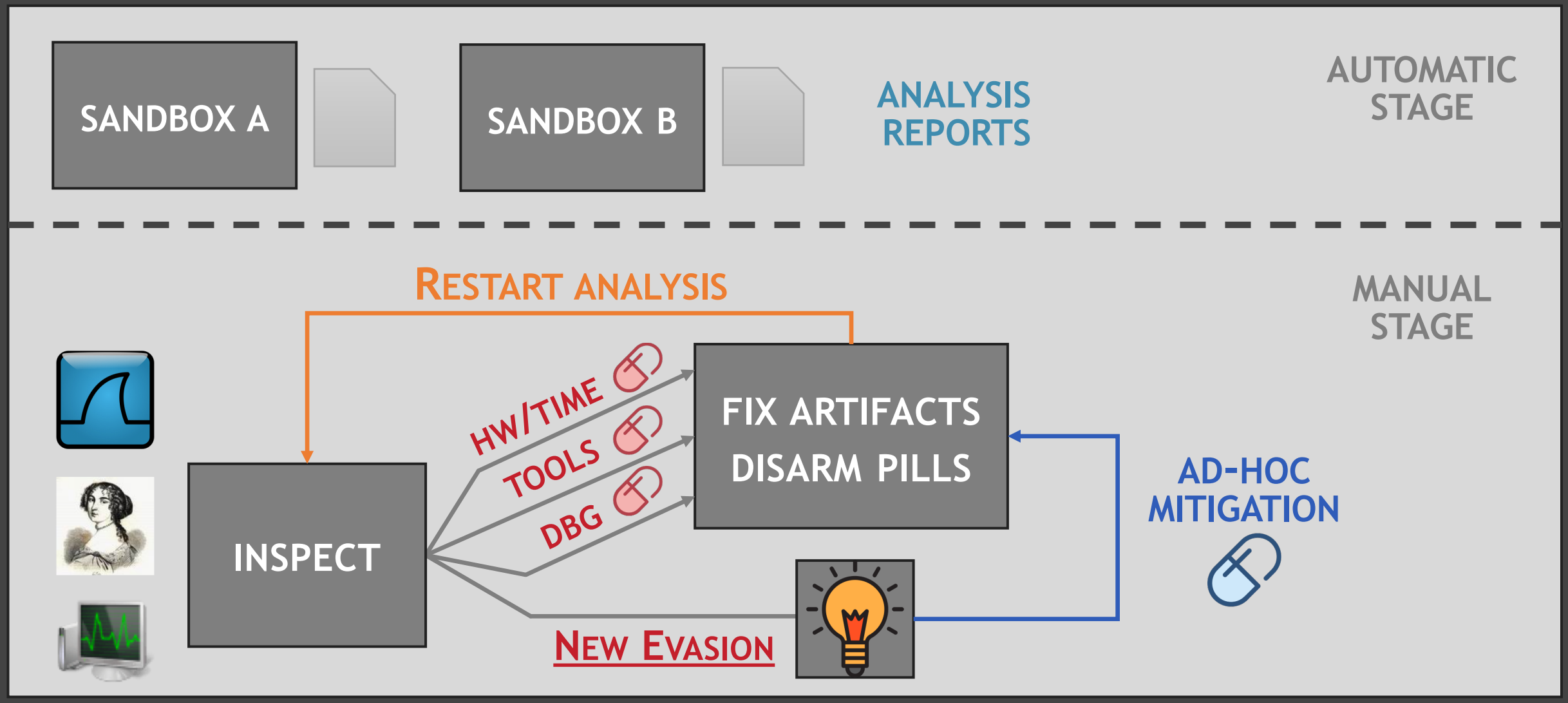
WHAT IF ANALYSTS COMMANDEER THEM?

- surgical use on points of interest spotted during dissection
- case study on taint analysis

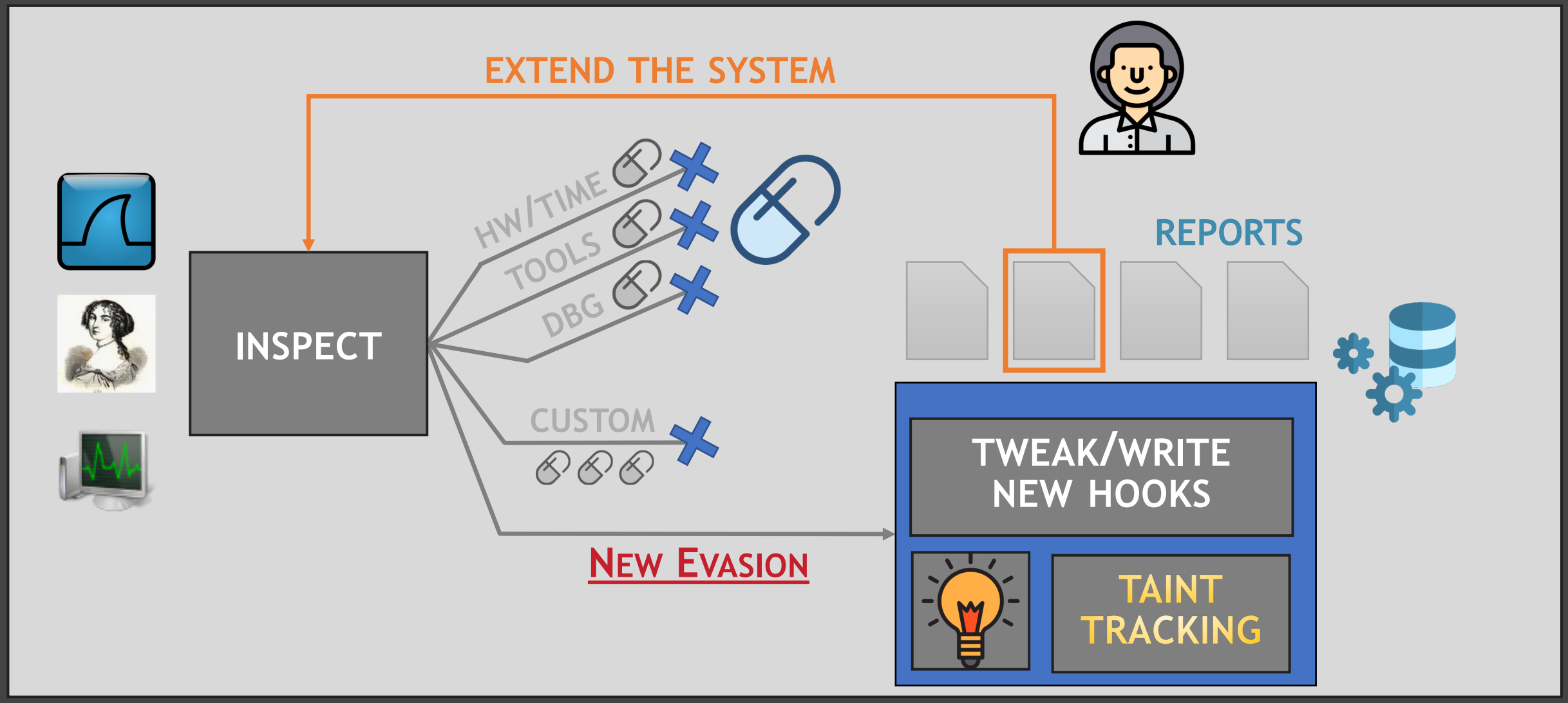
IN THIS TALK

- What we did
- Methodology
- Using BluePill

DISSECTION NOW



WITH BLUEPILL



PLAYGROUND

How we trained (for) BluePill

- tools: Al-Khaser, SEMS, VMDE, lots of PoCs for red pills
- protectors like VMProtect, Themida, Enigma, PELock
- complex samples with exotic evasions

WHAT HAPPENS WHEN YOU EVADE BLUEPILL?

- designed to favor extensions
- we gave CS students notable evasive malware

FURTIM

Performs over 400 adversarial checks

- few vendors could handle it when it came out
- early exit on VM/sandbox, plays with analysts when it spots one!

WE ASKED STUDENTS TO EXTEND BLUEPILL FOR FURTIM

- one hook missing wrt evasions from SentinelOne report
- one undocumented evasion with EnumDisplaySettings

FURTIM

```
void NtEnumerateKey_HookEntry(syscall_t *sc, ...) {
    KEY_INFORMATION_CLASS cl =  sc->arg2;
    if (cl == KeyBasicInformation) {
        PKEY_BASIC_INFORMATION str = sc->arg3;
        if (wcsstr(str->Name, L"VBOX") != NULL) {
            size_t nameLen = wcslen(str->Name);
            memcpy(str->Name, RANDOM_KEY_WSTR(nameLen), nameLen) }
   }
}
```

Taint tracking on NtQuerySystemInformation output revealed uses of wide-char string helpers. Hooking them revealed "VBOX" strings, and manual analysis spotted those as output from NtEnumerateKey.

FURTIM

```
void NtUserEnumDisplayDevices_HookExit(syscall_t * sc, …) {
    PDISPLAY_DEVICE disp = sc->arg2;
    WCHAR* devID = (UINT32)disp + 0x148;
    WCHAR* devString = (UINT32)disp + 0x44;
    WCHAR* devName = disp->DeviceName;

    if (wcsstr(devID, L"DEV_BEEF")) memset(deviceID, 0, …);
    if (wcsstr(devString, L"VirtualBox")) memset(devString, 0, …);
    if (wcsstr(devName, L"DISPLAY1")) memset(devName, 0, …);
}
```

for VirtualBox graphics adapter driver

NEXT STEPS

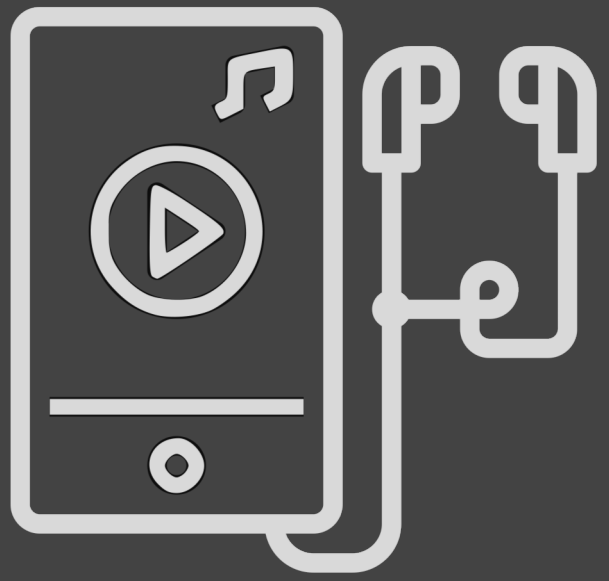
What we would like to do

- extensions for other analysis tasks
- explore how much can be ported to VMI
- get feedback from the community!

«On the dissection of evasive malware»

Daniele Cono D'Elia, Emilio Coppa, Federico Palmaro, Lorenzo Cavallaro, Camil Demetrescu

BLACK HAT SOUND BYTES



- Analysts aren't cheap: time spent disarming evasions should be put to a better use
- Providing fake answers is not new, but doing it right can be tricky
- DBI still good if you take proper precautions

https://github.com/season-lab/bluepill/

@dcdelia