Applying DevOps Principles for Better Malware Analysis

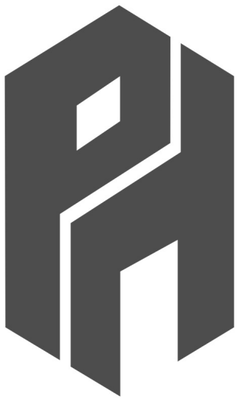
Olivier (@obilodeau)

- Cybersecurity Researcher at GoSecure
- Previously
  - Malware Researcher at ESET
  - Infosec lecturer at ETS University in Montreal
  - Infosec developer, network admin, linux system admin
- Co-founder Montrehack (hands-on security workshops)
- VP Training and Hacker Jeopardy at NorthSec

nsec

Hugo (@hugospns)

- Computer engineering student @ PolyMTL
- Director @ PolyHack
- Co-chapter leader (Audio, Recording and Streaming) @ OWASP Montreal
- Member of Jose Fernandez's SecSI lab @ PolyMTL
- Vulnerability Research Intern @ Wurldtech
- Former Intern @ ESET



Agenda

- Why?
- What?
- Where?
- Say whaat!?

Demo

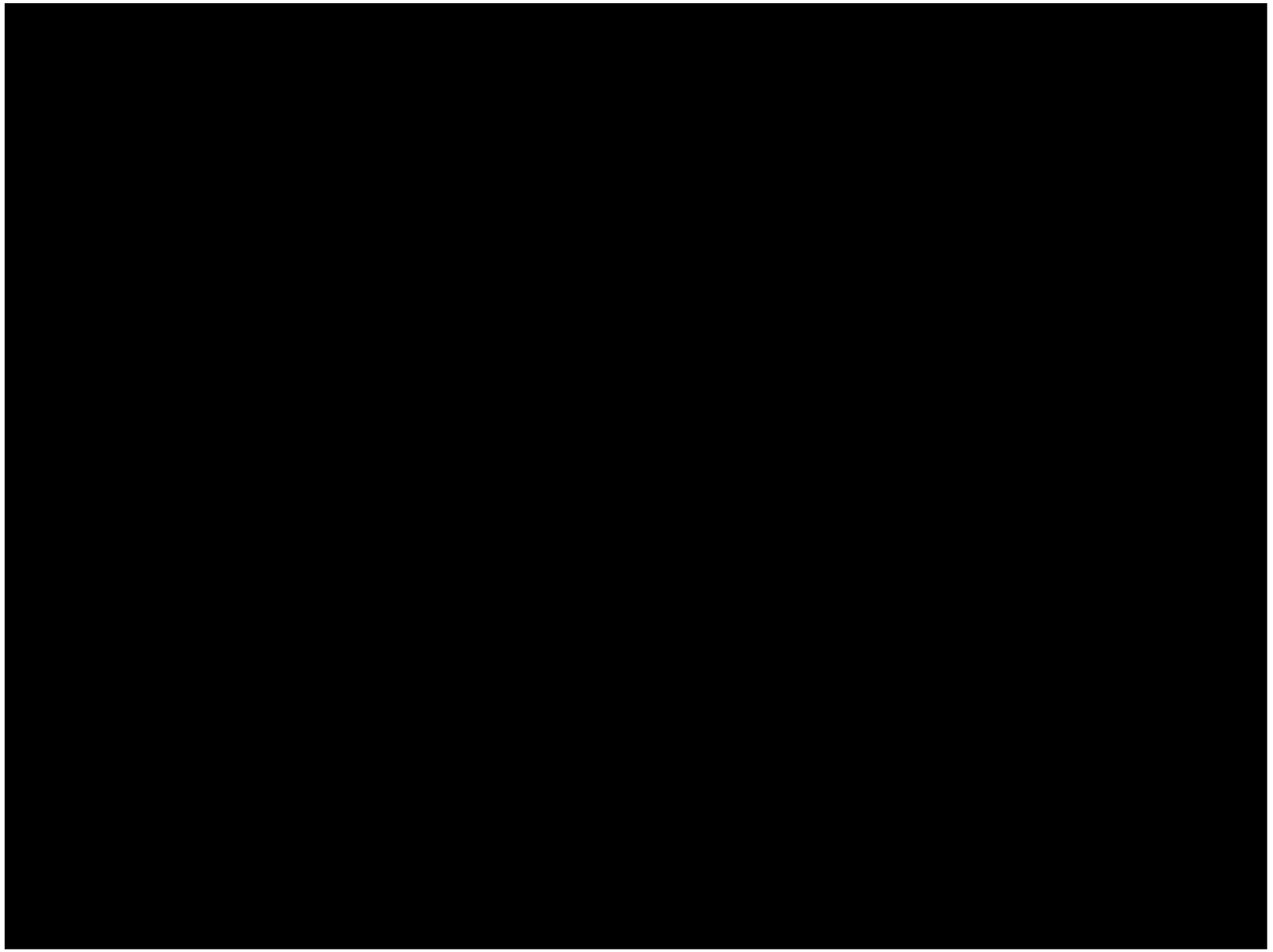
- Our demo

Questions?

```
@obilodeau
@hugospns
```

Why?

Context



Current toolchain (customization)

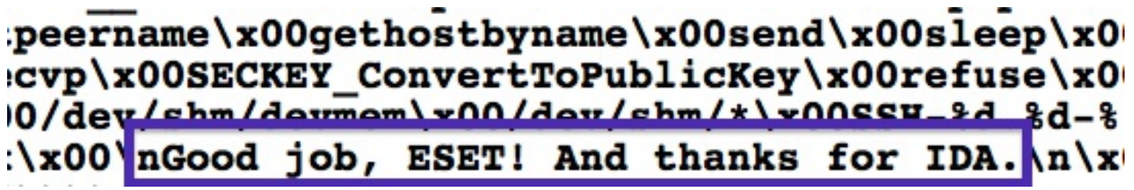
- Vanilla XP VMs (or more recent versions)
- No trace of a previous user
- Manual customization
- Can lead to cross-infected VMs
- Can’t build or reuse templates
- Also time consuming

The 90’s called and they want their methodology back

Problems of malware analysis

- Not accessible to newcomers
- Easy to mess things up
- Team work is hard (tools don’t encourage it)
- Building a credible environment is time consuming

Ways to mess things up



Also, dealing with VM problems

Analysis Detection

- Malware is doing analysis detection
- Anti-VMs like red pill, sldt instruction
  - Not reliable on multicore systems or when acceleration is deactivated.

Analysis Detection (cont.)

- Anti-debugging
  - Debugger plugins
- System fingerprinting
  - What is really available ?

One shot, one kill

- One chance to get noticed as interesting or else its too late
  - Your IP could be banned
- Has to be credible

What?

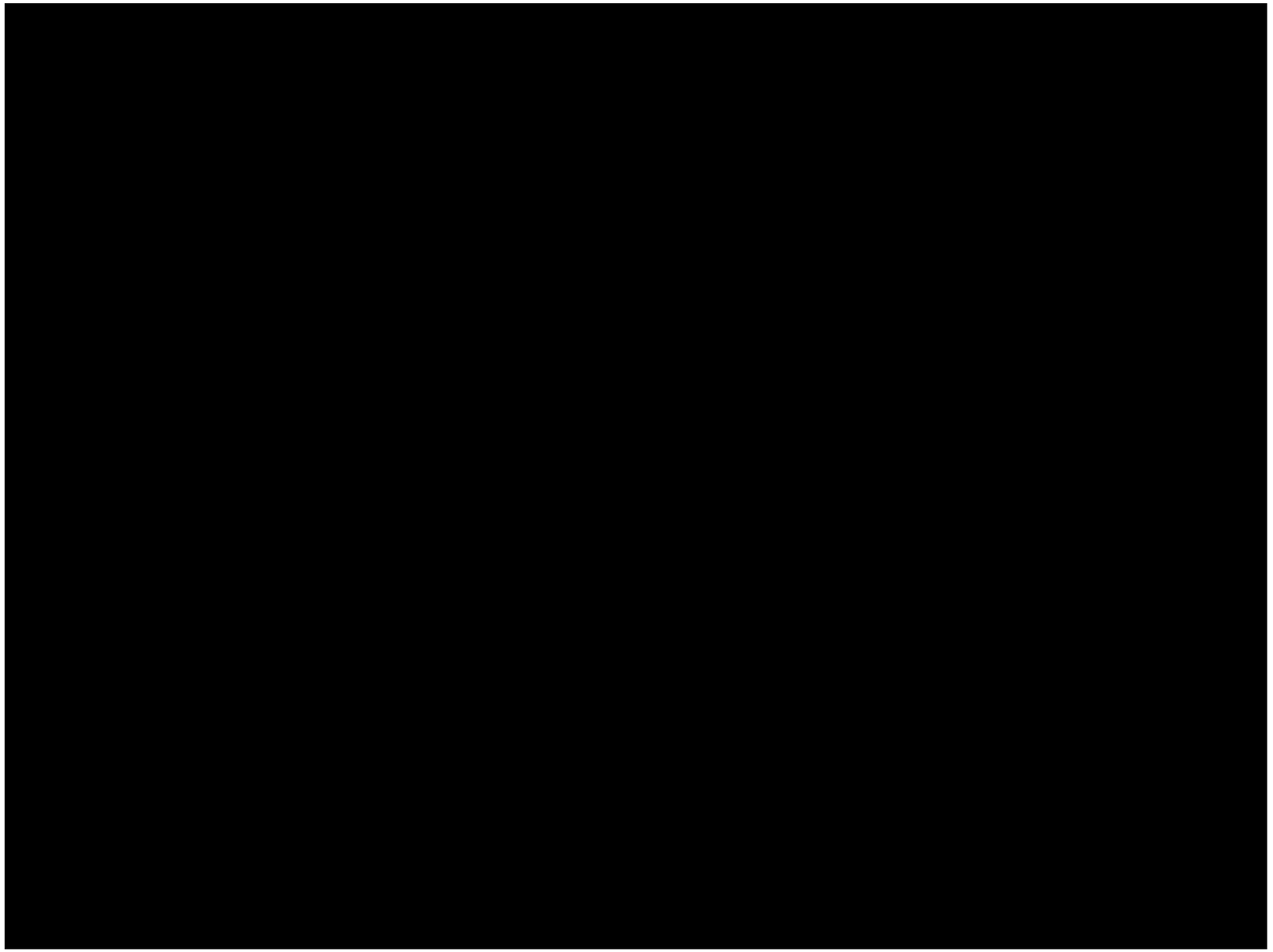
DevOps

Why would the devops people have all the fun?

DevOps (cont.)

- Core principle: Infrastructure as code
- Reproducible
- Throw-away
- Efficient

Inspiration



Architecture

- Reusing existing devops tools
  - packer: machine image builder
  - vagrant: configure reproducible operating environments
  - WinRM: Windows Remote Management

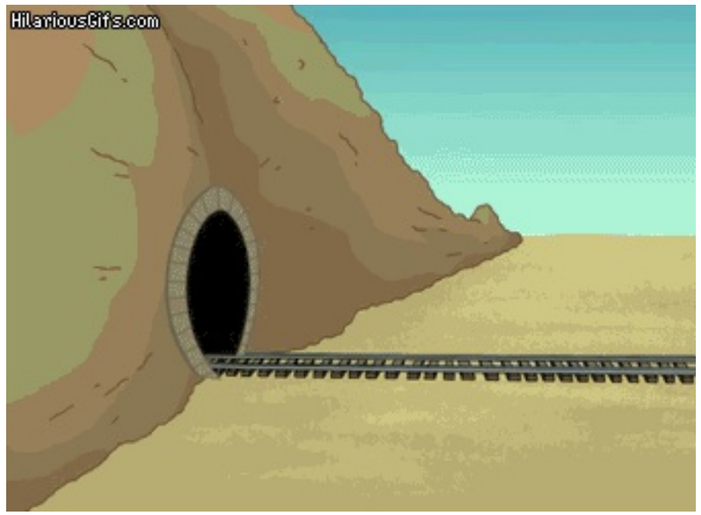
Shoulder of giants

- 2 years ago this wasn’t possible
- Borrowed some configs from Mark Andrew Dwyer’s packer-malware
- Chocolatey
- Hashicorp tools and community

Efficiency

- Tools automatically installed based on profiles
  - all sysinternal tools
  - windbg
  - putty
  - fiddler
  - wireshark

Dealing with VM problems



Malware in context

- Malware behaves differently in different contexts
- You know the target of the APT you are tracking and you want to fool them
- In as little time as possible

Use Cases

Win32/Syndicasec

- Manual recon
- Lists:
  - Last opened files
  - Directories
  - What’s on the Desktop
  - Systeminfo
    - Useful for: User, install date, hardware info

Operation Fingerprinting

- UNC / Shared drives fingerprinting
- Active Directory fingerprinting

Team analysis

Left as an exercise to the reader

How can I get this?

Anti-Vaporware Statement

```
git clone https://github.com/GoSecure/malboxes.git
```

How does it work?

- You use malboxes.py to build a profile
- Then it builds a `vagrant box` for you
- And you spin a `Vagrantfile` for each of your analysis

Available commands

- Registry - Modifies the Windows Registry (add, modify, delete)
- Document - Add or delete a file
- Directory - Add or delete a directory
- Package - Adds a Chocolatey package to install
- Build - Build the virtualbox image
- Spin - Create a `Vagrantfile` for your analysis case

Result

Useful for

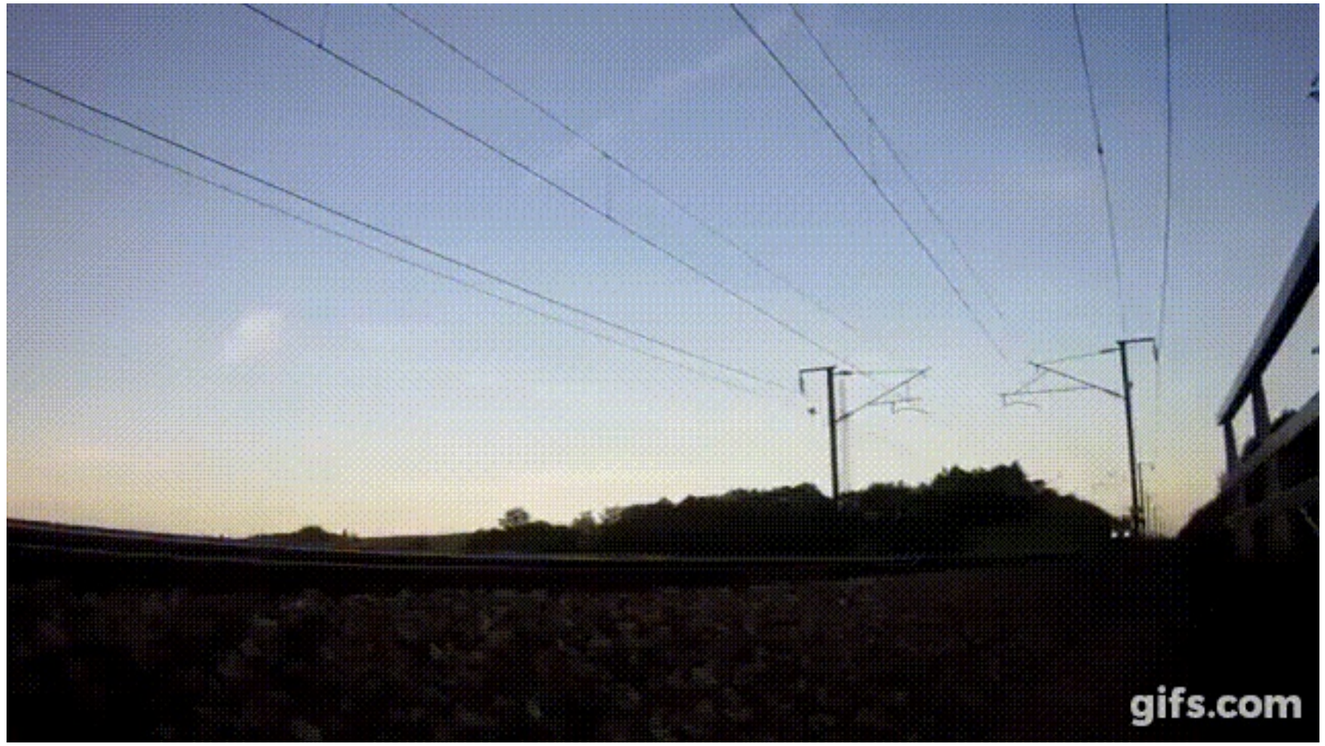
- Reduce art, augment science
- Get new people into malware analysis
- Improve workflow of seasoned analyst/teams

Where?

Where is this headed?

- Implement anti VM-detection tricks
- Higher level constructs to build interesting targets
  - Active Directory integration
  - Generate random honeydocs based on a theme
- Document a proper team workflow
- It’s all in `TODO.adoc`
- Join the fun!

Let’s get to work!



Thanks!

- Joan Calvet for tips and help
- Marc-Etienne M. Leveille for suggestions and link to Olivier
- Jurriaan Bremer for help with VMCloak
- Jose Fernandez and the lab team for tips and sponsorship
- Jessy Campos for pushing me
- My family, friends and girlfriend for support

Questions?

```
@obilodeau
@hugospns
```