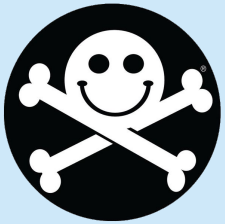


Telefónica Tech

KRAKEN

A MODULAR MULTI-LANGUAGE “WEBSHELL”

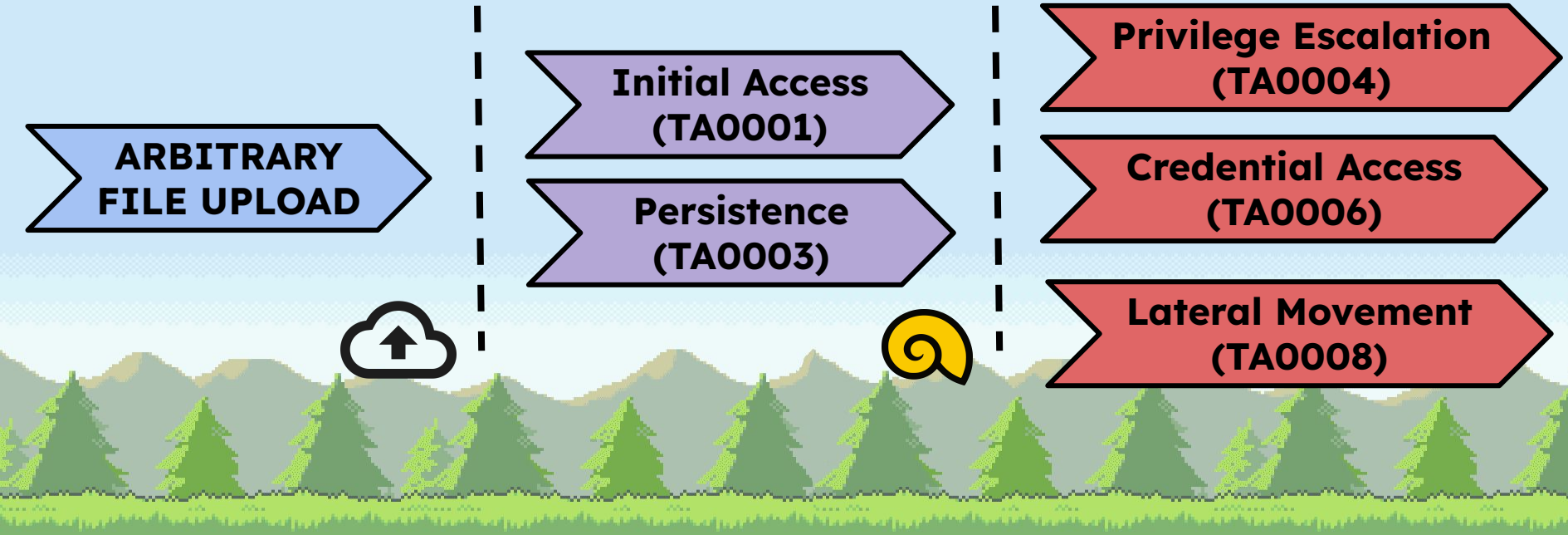
FOR DEFENSE EVASION

RAUL CARO TEIXIDO
(@secu_x11)

> whoami

- Raúl Caro Teixidó (aka **Secu**)
- **Offensive Security Engineer (Telefonica Tech)**
- Co-creator of **Mística** (4 covert channels)
- Twitter: [@secu_x11]
- Linkedin: [raul-caro-teixido]
- Blog: [https://makemalware.com]

Once upon a time...



Telefónica Tech

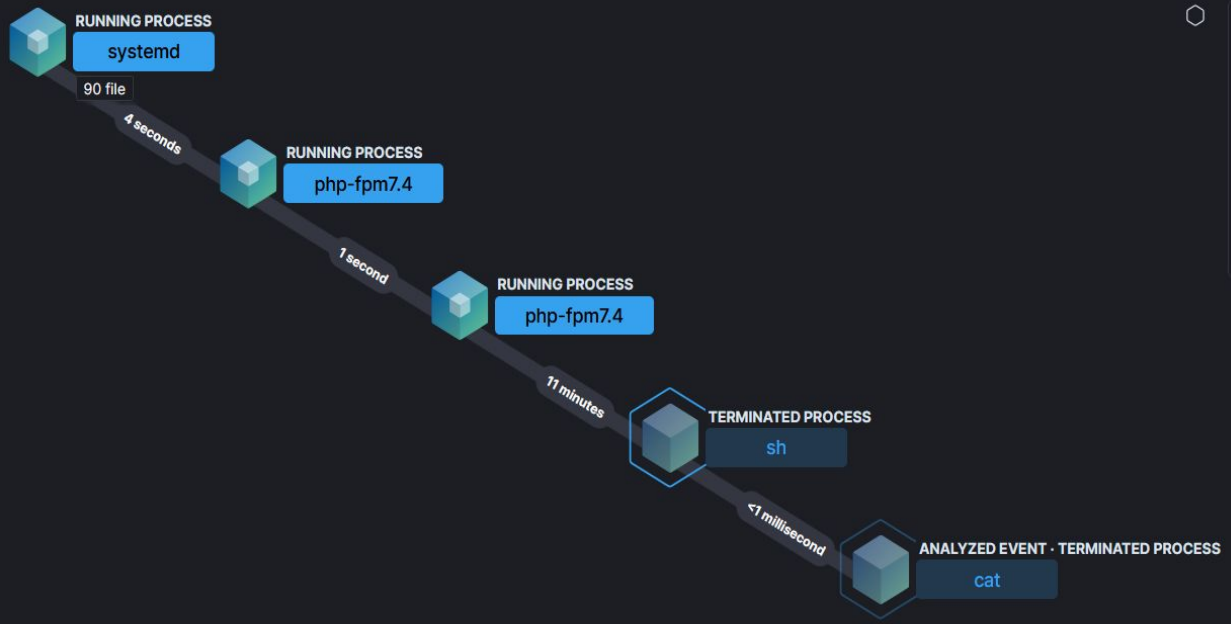
What happens when you run a webshell on a monitored computer?

sh

Terminated Process

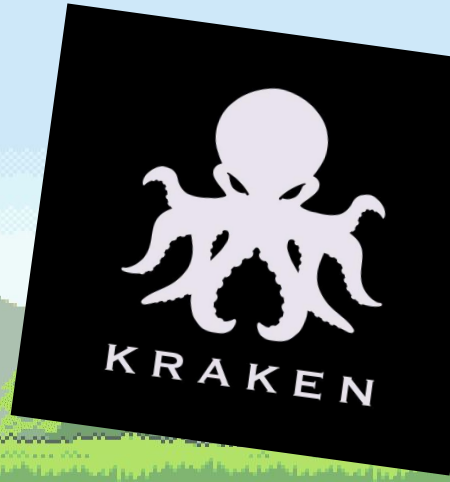
0 Events

@timestamp	Nov 24, 2022 @ 20:13:57.154
process.executable	/bin/sh
process.pid	3955
process.entity_id	ZmMyYjAxNzUtMDE2N
user.name	www-data
process.parent.pid	1012
process.hash.md5	7409ae3f7b10e059ee7
process.args	sh
process.args	-c
process.args	cat /etc/passwd 2>&1



What is Kraken?

- Webshell Orchestrator (**PHP, JSP, ASPX**)
- Framework for post-exploitation via Web
- A project focused on **Defense Evasion**
- **Multi-version** (backward compatibility)
- **Useful and comfortable TTY** (and more)



https://github.com/kraken-ng/Kraken

What are the benefits of Kraken over other tools?

Main Features (I)

- Avoids executing system commands, evading:
  - **Blocking Policies**
  - **AV/EDR/Security Solutions**
  - **Layer 7 Firewalls**

Main Features (II)

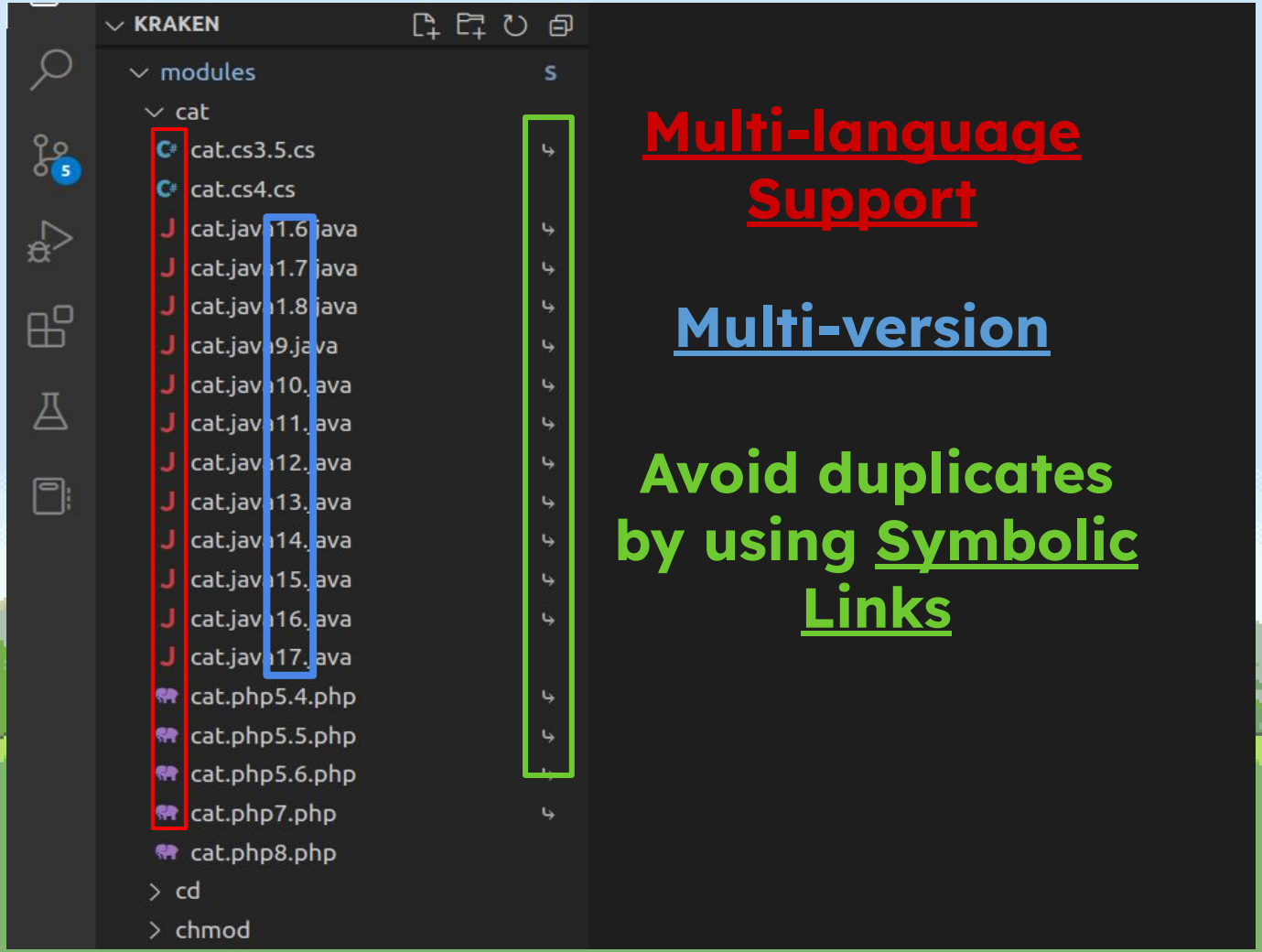
Use of **Token Leaks** in Windows (NET Agents)

- We can impersonate users:
  - At process level **(primary tokens)**
  - At thread level **(impersonation token)**
- And keep the security context of the token leaked because it stays in our process and can be used.

(*) Using an impersonation token, the Kraken modules executed will take the impersonated security context.

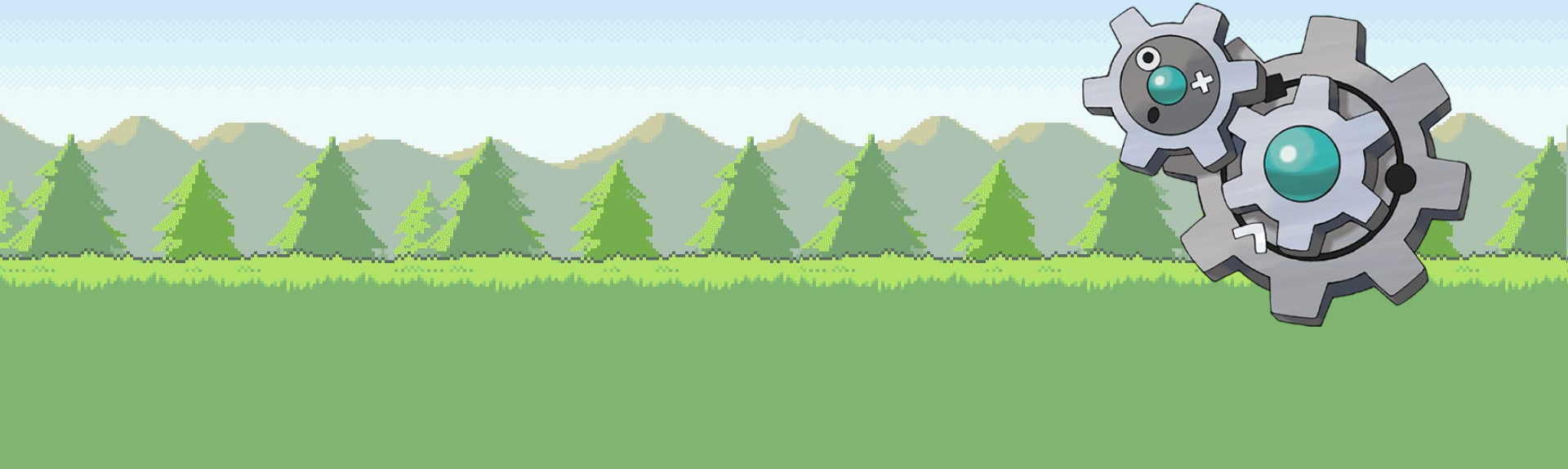
Main Features (III)

- Linux: everything is a file (processes, networking, etc)
- Windows + NET: a lot of juicy things!
  - **P/Invoke** (use unmanaged libraries)
  - **.NET libraries and functionalities.**
  - **Communicate with WMI, SMB and more...**



Telefónica Tech

How are Kraken modules loaded by Agents?



Executors

The executor is the Kraken Agent component, responsible for **invoking/evaluating/loading** the modules it receives from the client.

PHP	JSP	ASPX
eval()	ClassLoader	CSharpCodeProvider
create_function()	javax.tools.JavaCompiler	Assembly.Load()
include() / require()		System.Reflection.Emit

(not yet)

DEMO TIME!

THANK YOU!
AND THROW YOUR QUESTION!