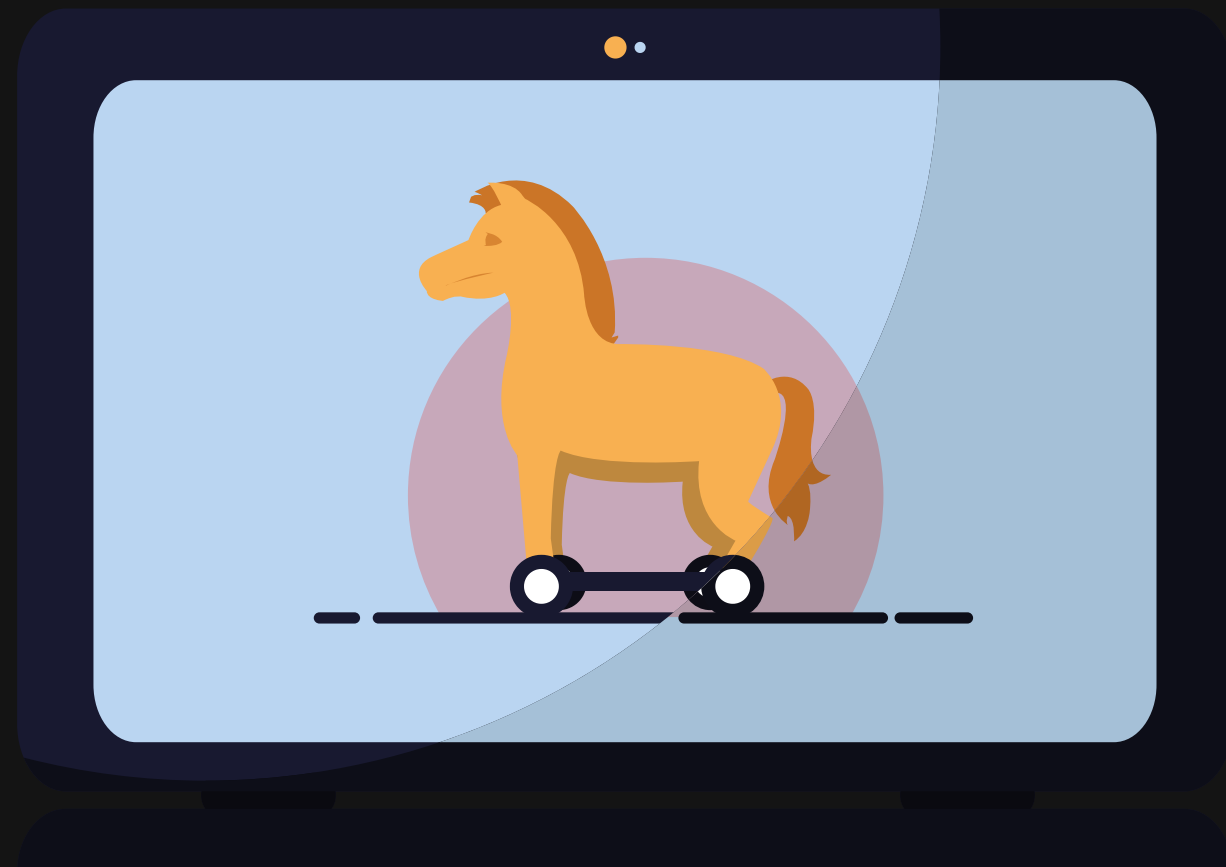


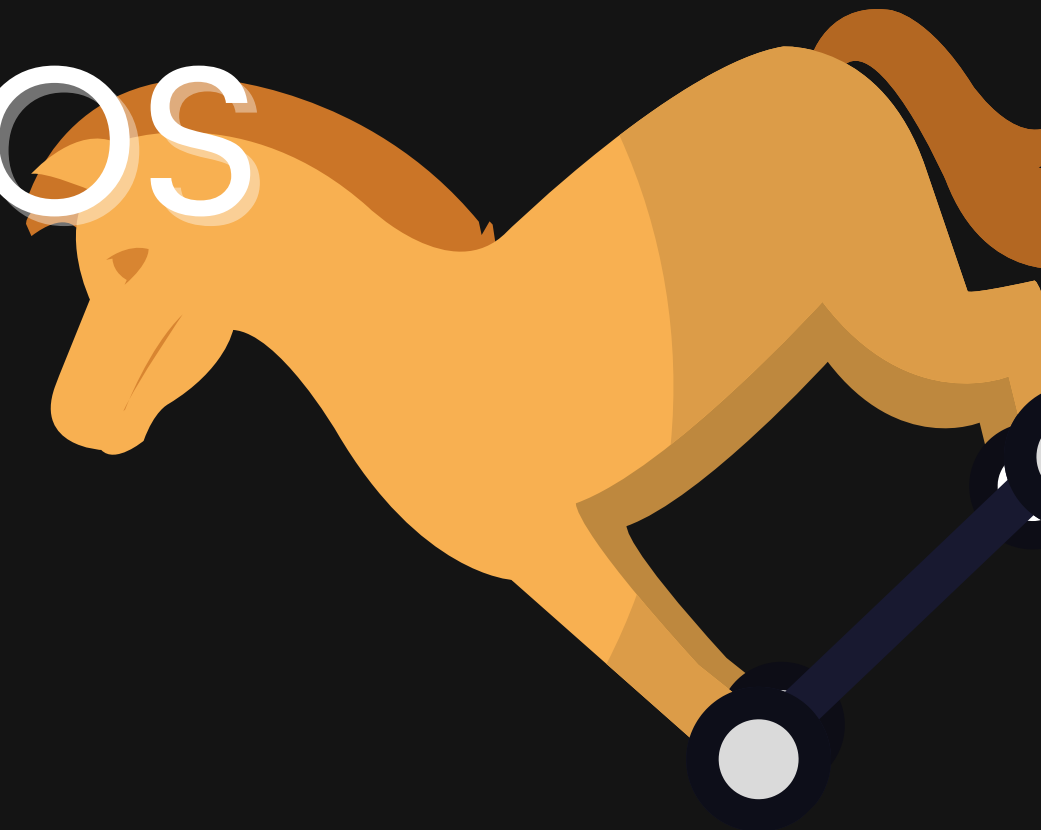
# Ataque a departamentos financieros en los Balcanes utiliza un backdoor y un RAT



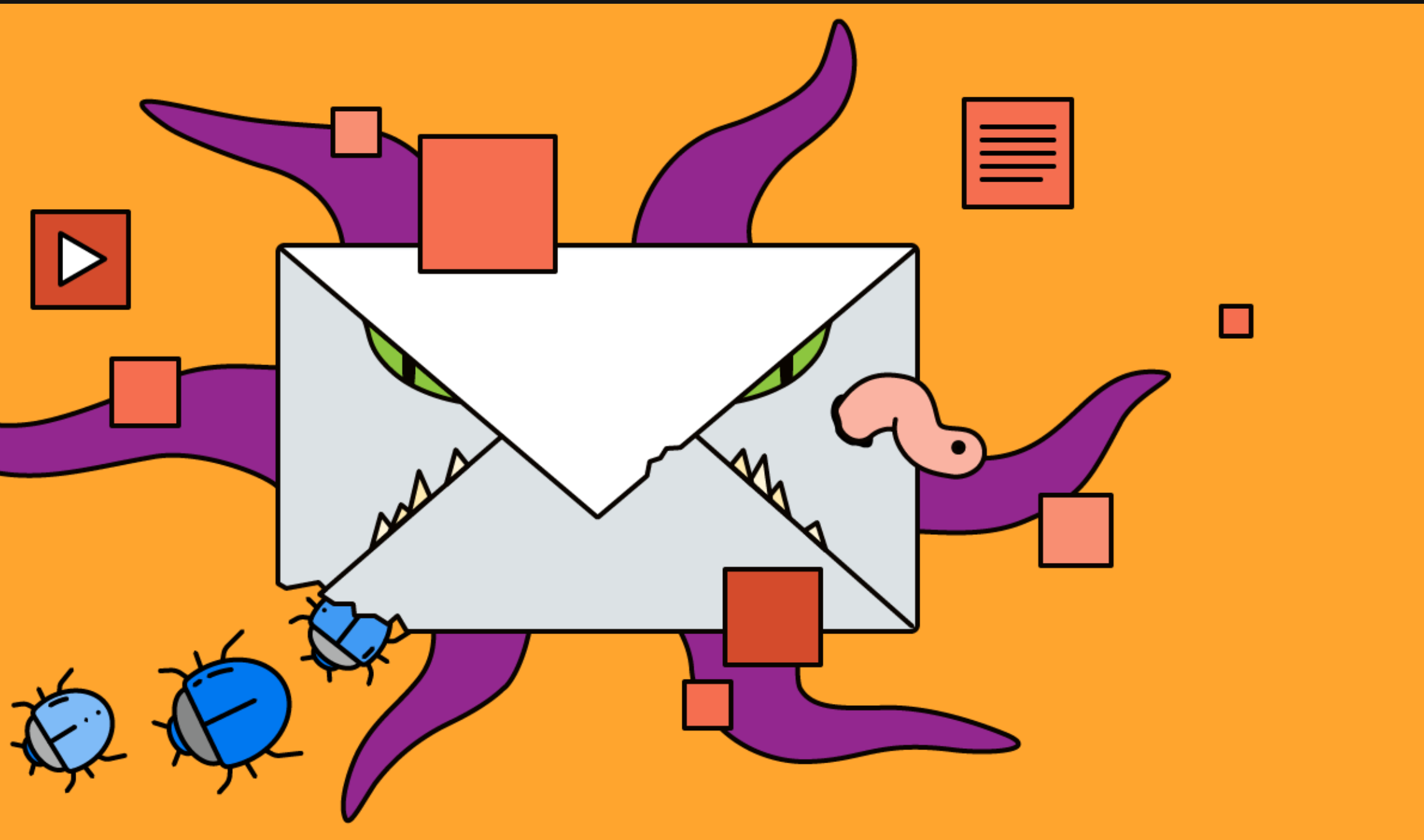


¿Qué tipo de  
amenaza es?

TROYANOS



# ¿Cómo comienza y cómo se propaga esta amenaza?



**Los malwares  
se distribuían  
vía Mail**

# ¿Hay más de una amenaza aplicada?

BACKDOOR

BalkanDoor



Imitan la identidad de sitios web  
legítimos de instituciones oficiales



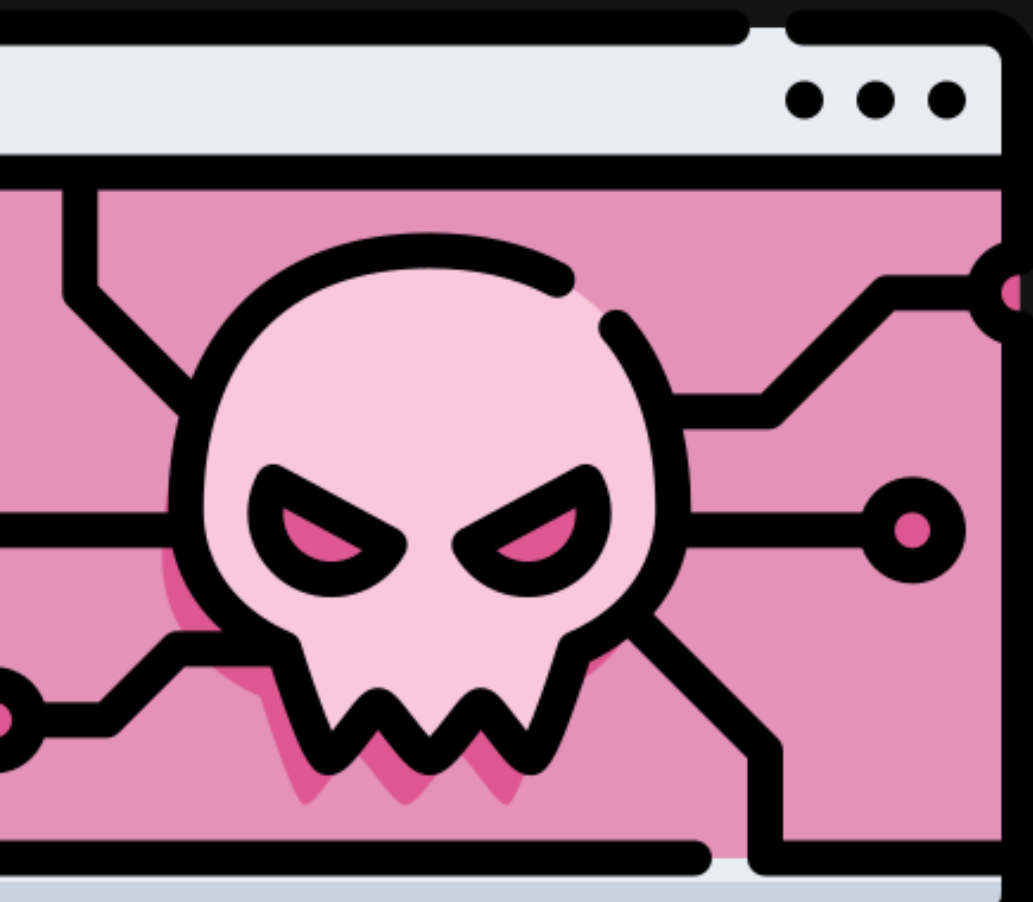
TROYANO DE ACCESO  
REMOTO (RAT)

BalkanRAT.



# ¿Como funcionan?

Ambas herramientas han sido desplegadas en la misma máquina. La combinación de las herramientas le brinda al atacante una interfaz de línea de comando y una interfaz gráfica para la computadora comprometida.



**Los PDF señuelo giran en torno al tema impositivo.**

# El tema del Mail eran los impuestos

Se cree que tenía  
motivos  
FINANCIEROS,  
no de espionaje



# Solución o medidas a tomar

Hay que tener en cuenta que estos malwares se disfrazan en mails que generalmente son enlaces a un PDF.

Table 1. Domains misused in the campaign		
Malicious domain	Real domain	Institution
pksrs[.]com	<a href="#">pks.rs</a>	Chamber of Commerce and Industry of Serbia
porezna-uprava[.]com	<a href="#">porezna-uprava.hr</a>	Ministry of Finance of Croatia, Tax Administration
porezna-uprava[.]net		
pufbih[.]com	<a href="#">pufbih.ba</a>	Tax Administration of the Federation of Bosnia and Herzegovina

- **NUNCA** clickear en links que nos llegan en el cuerpo de mails, salvo que estemos realizando una registracion.
- Tener un antivirus actualizado
- Mantener el sistema operativo actualizado
- Verificar el dominio del remitente del correo, si es malicioso suele notarse.