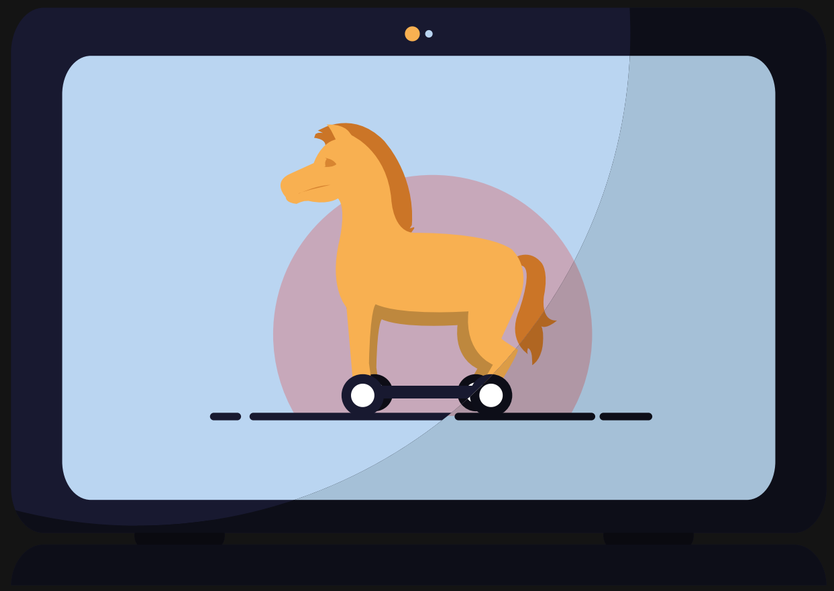
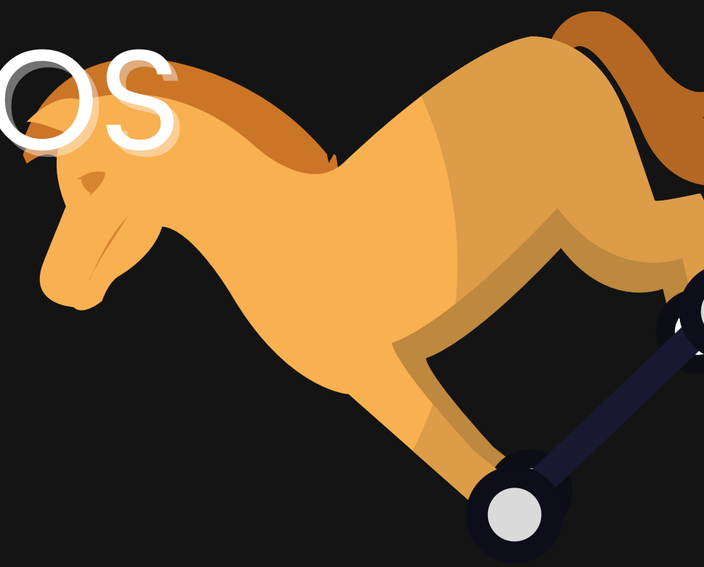
Ataque a departamentos financieros en los Balcanes utiliza un backdoor y un RAT

troyano

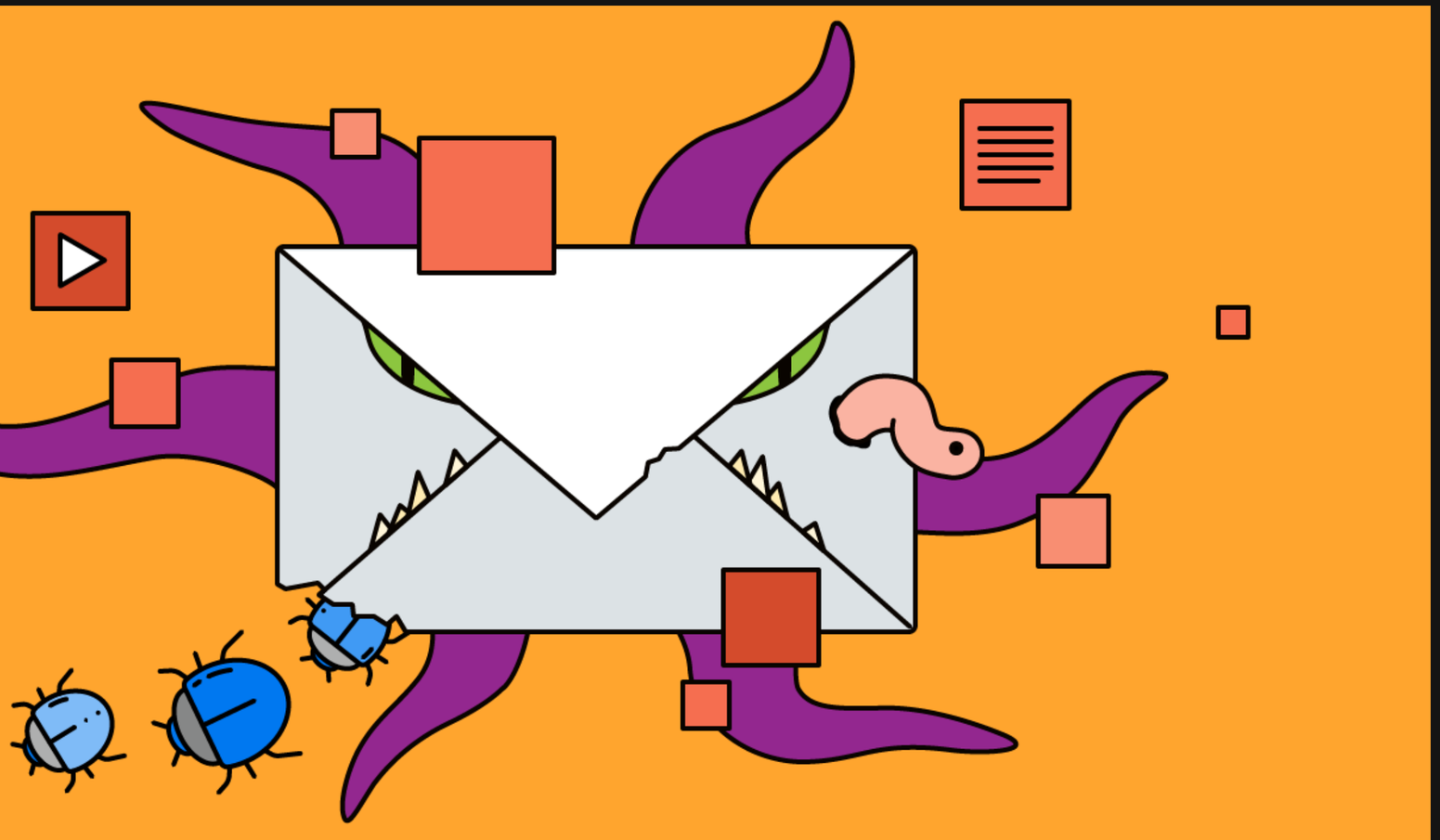


¿Qué tipo de amenaza es?

TROYANOS



¿Cómo comienza y cómo se propaga esta amenaza?



Los malwares se distribuian vía Mail

¿Hay más de una amenaza aplicada?

BACKDOOR

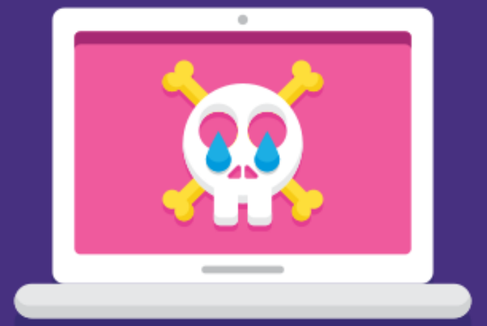
TROYANO DE ACCESO REMOTO (RAT)

BalkanDoor

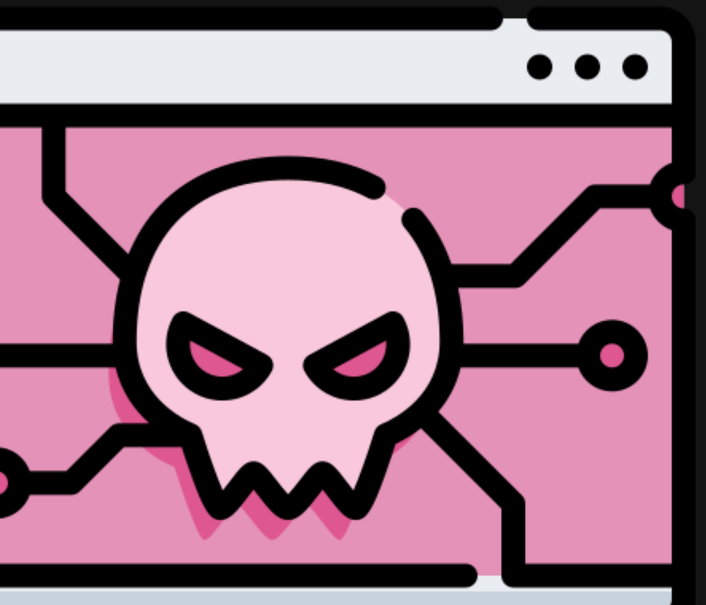
BalkanRAT.

Imitan la identidad de sitios web legítimos de instituciones oficiales

¿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.



El tema del Mail eran los impuestos

Se cree que tenia motivos FINANCIEROS, no de espionaje

Solución o medidas a tomar

Table 1. Domains misused in the campaign

Malicious domain	Real domain	Institution
pksrs[.]com	pks.rs	Chamber of Commerce and Industry of Serbia
porezna-uprava[.]com porezna-uprava[.]net	porezna-uprava.hr	Ministry of Finance of Croatia, Tax Administration
pufbih[.]com	pufbih.ba	Tax Administration of the Federation of Bosnia and Herzegovina

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

- 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.