

## Mesa 6

Nota : <<https://www.welivesecurity.com/la-es/2019/08/23/ataque-departamentos-financieros-balcanes-utiliza-backdoor-rat/>>

**¿Qué tipo de amenaza es?**

Malware, de tipo troyano.

**¿Cómo comienza y cómo se propaga esta amenaza?**

Comienza con email (phishing), se registra bajo el nombre de algún servicio y empieza a ejecutar scripts, se conecta a un servidor y solicita comandos.

## Mesa 6

Nota : <<https://www.welivesecurity.com/la-es/2019/08/23/ataque-departamentos-financieros-balcanes-utiliza-backdoor-rat/>>

### ¿Hay más de una amenaza aplicada ?

Si, 2 normalmente una técnica de backdoor y otra de acceso remoto, suelen nombrarlos como BalkanDoor y BalkanRAT

### ¿Qué solución o medida recomendarían ?

No abrir correos sospechosos, examinar los archivos y enlaces adjuntos, y mantener actualizados los equipos y los sistemas de seguridad