* Que tipo de amenaza es?

Es un troyano llamado puerta trasera, es una secuencia especial o un término trasero dentro del código de programación, mediante la cual se pueden evitar los sistemas de seguridad del algoritmo para acceder a la misma.

* Como comienza y se propaga?

Las puertas traseras se introducen en el sistema gracias a otros programas nocivos como [troyanos](https://www.pandasecurity.com/es/security-info/trojan/), [virus](https://www.pandasecurity.com/es/security-info/virus/) o incluso spyware. Consiguen acceso sin que el administrador se de cuenta y luego infectan las sesiones a cada uno de los usuarios conectados a la red comprometida. Es posible que algunas amenazas puedan ser colocadas con carácter previo por usuarios que tienen los privilegios adecuados, para ganar acceso más tarde.

Ciertas backdoors se integran en aplicaciones específicas. En ocasiones programas legítimos pueden tener vulnerabilidades no documentadas que permiten el acceso remoto. En estos casos los atacantes siguen necesitando alguna forma de entrar en contacto con el equipo afectado para obtener inmediatamente un acceso no autorizado al sistema.

Los propios usuarios pueden instalar accidentalmente puertas traseras en sus ordenadores sin darse cuenta. Un virus de puerta trasera puede venir adjunto a aplicaciones de intercambio de archivos o mensajes de correo electrónico. A veces utilizan técnicas análogas a las del [scareware](https://www.pandasecurity.com/es/security-info/scareware/) y el [ransomware](https://www.pandasecurity.com/es/security-info/ransomware/).

Algunas puertas traseras pueden utilizarse mediante la explotación de sistemas remotos con vulnerabilidades de seguridad específicas, en los equipos o la red.

* Hay mas de una amenaza aplicada?

No, solo un troyano.

* Que solución o medida recomendarían?

Recomendaria invertir en buenos sistemas anti-malware que ofrezcan tecnologías de antivurs, troyanos, fishing, backdoors, ramsomware y un back up semanal.