Respuestas:

Los ataques fueron mediante 1 backdoors y 1 troyano.

2 y 3-

BalkanRAT permite al atacante controlar remotamente la computadora comprometida a través de una interfaz gráfica, es decir, manualmente; mientras que BalkanDoor permite controlar de forma remota la computadora comprometida a través de una línea de comando; ambas utilizadas de manera grupal.

En este caso se trato de una típica víctima de esta campaña, la cual utiliza correos electrónicos maliciosos como mecanismo de distribución, termina teniendo ambas herramientas implementadas en su computadora, cada una de ellas capaz de controlar totalmente la máquina afectada. Esta configuración poco común hace que sea posible para los atacantes elegir el método más adecuado para indicarle a la computadora que lleve adelante las operaciones de su elección.

Los atacantes distribuyeron sus herramientas a través de correos electrónicos maliciosos (“malspam”) con enlaces que conducen a un archivo malicioso.Los enlaces incluidos en los correos de malspam y fueron utilizados para la distribución de BalkanRAT y BalkanDoor, imitaron la identidad de sitios web legítimos de instituciones oficiales.

**BalkanDoor** y **BalkanRAT**. el primero se ejecuta como un servicio de Windows, lo que le permite desbloquear la pantalla de inicio de sesión de Windows de forma remota y sin la contraseña o iniciar un proceso con los privilegios más altos posibles. En el caso de BalkanRAT utiliza indebidamente un software de escritorio remoto (RDS) legítimo y utiliza herramientas adicionales y scripts para ocultar a la víctima su presencia, como ocultar la ventana, el icono de la barra de tareas, el proceso, etc.

--Extra

El ataque por medio de backdoors se produce como un ataque como su nombre lo dice de puerta trasera, este es un tipo de troyano. Los backdoors puros pueden venir previamente instalados en el sistema o aplicaciones utilizadas por el usuario, ya sea porque los desarrolladores se les olvidó quitar o bloquear esa función o se dejó así a propósito.

El troyano es un malware que se presenta al usuario como un programa aparentemente legitimo e inofensivo, pero que al ejecutarlo, le brinda al atacante acceso remoto al equipo infectado.

En un *backdoor*, es importante diferenciar entre aquellos que se intentan instalar en nuestro sistema (fundamentalmente utilizando troyanos) y los que vienen ya incluidos en él o en alguna aplicación de confianza.

4-

Los productos de seguridad de ESET detectan estas amenazas como Win{32,64}/BalkanRAT y Win32/BalkanDoor.

--Extra

Los primeros son **relativamente fáciles de eliminar**, puesto que un [análisis del tráfico](https://www.welivesecurity.com/la-es/2015/01/21/como-crear-perfiles-de-red-monitorear-trafico/) de nuestra red o incluso del propio binario puede sacar a la luz funcionalidades no deseadas. Un antivirus actualizado o, si preferimos entrar nosotros mismos en materia, un análisis profundo con una herramienta de desensamblaje pueden revelar funciones ocultas de *backdoor* que no se ven a primera instancia.

El problema viene con aquellas aplicaciones o sistemas que lo llevan incluido en su sistema. En esos casos es cuando debemos confiar en la comunidad de usuarios que lo revisan, en el caso de utilizar *software* libre, o cruzar los dedos y confiar en las buenas intenciones de la empresa a la que hemos dado nuestra confianza.