Puertas de atrás (back doors)

* **Descripción de la amenaza**.

Un backdoor es cualquier método utilizado por usuarios tanto autorizados como no autorizados para evitar medidas de seguridad normales y conseguir alto nivel de acceso a un sistema informático, red o aplicación software.

A diferencia de otros ciberataques que son conocidos por hacerse notar (ej. Ransomware), los backdoors tienen la característica de que son discretos.

Pueden ser instalados en la víctima de dos maneras diferentes:

* Hardware/Firmware: alteraciones físicas que proporcionan acceso remoto al sistema.
* Software: archivos malware que esconden su rastro de manera que el sistema operativo no sabe que otro usuario está accediendo al dispositivo.

Son generalmente clasificados como un tipo de troyano. Cualquier malware que proporciona a los hackers(crackers) acceso a un sistema puede ser considerado como un backdoor, esto incluye: rootkits, troyanos, spyware, cryptojackers, keyloggers, gusanos y ransomware.

Para que un cibercriminal instale de manera exitosa un backdoor en el sistema víctima, primero tiene que conseguir acceso al dispositivo y esto puede hacerlo mediante acceso físico, un ataque malware, o con un exploit de una vulnerabilidad. Las vulnerabilidades más comunes que los atacantes abusan son las siguientes:

* Puertos abiertos.
* Contraseñas débiles.
* Software no actualizado.
* Firewalls de baja calidad.
* **Riesgos que supone**.

El atacante puede utilizar el backdoor para instalar todo tipo de malware en el sistema afectado:

* **Spyware**: registra información sobre la víctima, las páginas web que visita, las cosas que descarga, los archivos que abre, nombres de usuario y contraseñas y cualquier otra cosa de valor.
* **Ransomware**: un tipo de malware diseñado para encriptar los archivos de la víctima y/o bloquear el sistema. Para deshacer el problema, el atacante normalmente solicita dinero a la víctima.
* **Esclavo de ataque DDoS**: el atacante podría utilizar el sistema al que ha obtenido acceso para que forme parte de una botnet preparada para realizar un ataque DoS coordinado.
* **Cryptojacking**: los recursos del sistema víctima del backdoor son utilizados por el atacante para realizar minado de criptomonedas.
* **Medidas correctivas (para evitar la amenaza)**.
* **Adquisición de un nuevo producto**: dado que el departamento de TI ya no usará las contraseñas por defecto debido a la decisión de realizar un cambio interno, se recomienda adquirir un **gestor de contraseñas**. Los gestores de contraseñas generan y almacenan la información de sesión para todas las cuentas y ayudan a entrar en ellas de manera automatizada. Para que esto pueda realizarse de manera segura, la información se encripta mediante algún algoritmo como AES 256-bit y bloqueado tras una contraseña master.

Consideramos la adquisición de un gestor de contraseñas avanzado como Dashlane, que potencia la seguridad mediante la posibilidad de realizar un inicio de sesión biométrico o herramientas 2FA como generadores TOTP y tokens USB.

Ya que estos gestores avanzados generan contraseñas aleatorias y complejas, será mucho más difícil para un atacante acceder a la red o traspasar más allá de los primeros niveles.

* **Contratación de un nuevo servicio**: contratación de un antivirus avanzado y endpoint protection que incluyan en el servicio la protección contra vulnerabilidades zero day que no todos los servicios ofrecen, o la ofrecen solo con determinados niveles de suscripción.

Las vulnerabilidades zero day son las que han sido descubiertas muy recientemente y solo las empresas de seguridad más avanzadas han conseguido encontrar la solución para combatirlas, mientras que otras entidades apenas tienen conocimiento de la existencia de estas vulnerabilidades o aún no han descubierto como solucionarlas.

* **Ejecución de un cambio interno**: el departamento de TI nunca deberá usar la contraseña por defecto de un sistema adquirido.

Por otra parte, siempre se intentará utilizar el protocolo https para navegar por internet.

* **Ejemplos (casos reales) de back doors.**
* **WannaCry**: en 2017, se instaló a través de un backdoor el ransomware WannaCry que afectó a cientos de miles de sistemas.

Concretamente afectó a más de 230.000 ordenadores distribuidos en 150 países y se propagó mediante EternalBlue, un exploit desarrollado por la NSA para ordenadores Windows antiguos. Un grupo de hackers conocidos como Shadow Brokers robó EternalBlue, instaló el backdoor DoublePulsar y entonces encriptó los datos, demandando 600$ en bitcoin como pago para deshacer ransomware.

Como resultado del ataque, 19.000 reuniones fueron canceladas, costándole a la NHS 110 millones de euros. Alrededor del mundo, se estima que en total causó costes de aproximadamente 4 billones de dólares.

* **SolarWinds Sunburst**: el 14 de diciembre de 2020, backdoors maliciosos conocidos como Sunburst y Supernova fueron descubiertos en SolarWinds. Esta empresa es una de las más importantes de tecnología de información de EE.UU y se dedica a crear software que ayuda a las empresas a manejar sus redes, sistemas e infraestructura TI.

Los cibercriminales consiguieron acceso a los sistemas de SolarWinds de la sede de Texas y añadieron código malicioso en el software Orion, uno de sus softwares dedicado a la gestión de recursos.

Sin saberlo, SolarWinds envió actualizaciones del software Orion a sus clientes, que ya contenía el código malicioso. Cuando los clientes lo descargaron, se creó el backdoor en sus sistemas, y estos fueron usados para espiarlos.

SolarWinds reportó que 18.000 de sus 300.000 clientes fueron afectados por el backdoor del software Orion. Las pérdidas fueron de aproximadamente 90 millones de dólares, siendo este uno de los mayores ciberataques de la historia.