Check Point Software alerta: las cookies de sesión son una tentación irresistible para los ciberdelincuentes

Check Point Software estima que se robaron 22 mil millones de registros de cookies en 2022

Las cookies son una de las tecnologías web más importantes, aunque son casi tan antiguas como el propio navegador web. Check Point® Software Technologies Ltd. (NASDAQ: CHKP), proveedor líder en soluciones de ciberseguridad en la nube basadas en IA, alerta sobre cómo representan una oportunidad única para que los ciberdelincuentes puedan sustraerlas, con un cálculo estimado de robo de 22 mil millones de registros de cookies en 2022. En el caso de las aplicaciones SaaS de las empresas, pueden implicar el robo o mal uso de datos sensibles.

Las cookies de sesión de corta duración, como las generadas por sitios bancarios, no son particularmente atractivas pero las de duración más larga sí lo son, ya que se utilizan para sesiones "activas" y permanecen varias horas o días. Es importante tener en cuenta que las cookies de sesión se utilizan para autenticar la identidad de un usuario, lo que significa que se generan después de la autenticación multifactor (MFA). Así, el ciberdelincuente puede "pasar la cookie" o usarla para una nueva sesión web y hacerse pasar por un usuario legítimo.

Los atacantes pueden robar las cookies de sesión de diversas formas, como mediante el acceso a redes Wi-Fi no seguras, ataques de scripting entre sitios, phishing, troyanos y ataques man-in-the-middle. Un ejemplo real es el Racoon Stealer, una de las muchas familias de malware diseñadas para robar cookies. El grupo de piratas informáticos Lapsus$ utilizó Racoon Stealer para obtener acceso no autorizado a los sistemas de la empresa de videojuegos Electronic Arts utilizando una cookie de sesión robada. Crearon una cuenta clonada de un empleado real de EA y se hicieron con cientos de GB de datos, incluido el código fuente del juego.

En este sentido, Check Point Software destaca la importancia de mirar a través de una lente Zero Trust y expone dos medidas para mitigar la amenaza y evitar el robo de las cookies de sesión:

Defensa de aplicaciones SaaS
Una empresa utiliza de media 130 de aplicaciones SaaS. Estas cookies de sesión permiten el acceso a la misma información y permisos que el usuario legítimo (transacciones de ventas y archivos internos). En el caso de una sesión de correo web secuestrada, el ciberdelincuente podría acceder a todos los

correos electrónicos del usuario y hacer envíos que inciten a otros a tomar acciones específicas que le beneficien.

Afortunadamente, es posible -y bastante simple- defenderse contra los peligros de las cookies de sesión con Harmony SASE SaaS Protection. Asigna una dirección IP única y estática a la empresa, y solo permite el acceso a las aplicaciones Saas al tráfico proveniente de una dirección legítima. Todo lo demás se deniega por defecto, incluso si un atacante ha obtenido cookies de sesión activas que, nuevamente, evaden el mecanismo MFA. De esta forma, el servidor SaaS bloqueará el tráfico.

Protección más allá de la cookie de sesión
La fácil disponibilidad de SaaS implica un acceso cómodo para los miembros del equipo, estén donde estén, pero también les da a las atacantes oportunidades para buscar brechas de seguridad.

Además de una dirección IP única, Harmony SASE también permite alinear el acceso y los permisos de los usuarios con sus roles y responsabilidades. Esto mantiene a todos "en su sitio" y evita el acceso no autorizado a aplicaciones y datos.

Harmony SASE también proporciona visibilidad en tiempo real y reportes fáciles de los usuarios y dispositivos que se conectan a tus aplicaciones SaaS. "Si alguna vez tienes motivos para sospechar actividad no autorizada, un usuario y todos sus dispositivos pueden cerrar sesión con solo hacer clic en un botón. Esto también es útil cuando un empleado se va, ya que su acceso a todas las aplicaciones SaaS puede ser desactivado instantáneamente".

Se puede visitar la página Harmony SASE para obtener más información sobre la protección de sus aplicaciones SaaS.