Robo de ‘Cookies’, la nueva táctica de los hackers contra la autenticación multifactor

- *Sophos identificó que las cookies de sesión robadas por los ciber atacantes les ayudan a pasar por usuarios legítimos y moverse libremente por las redes vulneradas.*

CIUDAD DE MÉXICO. 23 de agosto de 2022.– Sophos, líder mundial en ciberseguridad de última generación, publicó un informe llamado "Robo de cookies: el nuevo desvío del perímetro", que los adversarios activos están utilizando cada vez más el robo de estos códigos y/o datos que se generan cuando un usuario inicia sesión dentro de una plataforma web, para eludir la autenticación multifactor (MFA) y obtener acceso a los recursos corporativos.

● ¿Cómo lo hacen?

En algunos casos, el robo de cookies en sí mismo es un ataque altamente dirigido, con adversarios que extraen datos de sistemas comprometidos dentro de una red y usan programas ejecutables legítimos para disfrazar la actividad maliciosa. Una vez que los atacantes obtienen acceso a los recursos corporativos basados en la web y en la nube utilizando las cookies, pueden usarlos para tener un mayor alcance, como el hecho de comprometer la red de correo electrónico comercial, la ingeniería social para obtener acceso adicional al sistema e incluso la modificación de los repositorios de datos o código fuente.

“Durante el año pasado, hemos visto a los atacantes recurrir cada vez más al robo de cookies para evitar la autenticación multifactor. Los atacantes están recurriendo a versiones nuevas y mejoradas de malware de robo de información como Raccoon Stealer para simplificar el proceso de obtención de cookies de autenticación, también conocidas como tokens de acceso”, dijo Sean Gallagher, investigador principal de amenazas de Sophos. *“Si los atacantes tienen cookies de sesión, pueden moverse libremente por una red, haciéndose pasar por usuarios legítimos”.*

● ¿Qué son las ‘cookies’?

Las cookies de sesión o autenticación son datos almacenados por un navegador web cuando un usuario inicia sesión. Si los atacantes los obtienen, pueden inyectar dicho token de acceso en una nueva sesión web, engañando al navegador para que crea que es el usuario autenticado y anulando la necesidad de autenticación.

Dado que un token también se crea y almacena en un navegador web cuando se usa MFA, este mismo ataque se puede usar para eludir esta capa adicional de autenticación. Para agravar el problema, muchas aplicaciones legítimas basadas en la web tienen cookies de larga duración que rara vez o nunca caducan; otras solo caducan si el usuario se desconecta específicamente del servicio.

Hoy en día, la industria del malware como servicio hace más fácil para los atacantes de nivel básico que se involucren en el robo de credenciales. Por ejemplo, todo lo que necesitan hacer es comprar una copia de un troyano que roba información como Raccoon Stealer para recopilar datos como contraseñas y cookies a granel y luego venderlos en mercados de cibercrimen. Otros, como los operadores de ransomware, pueden comprar estos datos y filtrarlos para aprovechar vulnerabilidades o exploits que encuentren y robar datos.

Por el contrario, en dos de los incidentes recientes que investigó Sophos, los atacantes adoptaron un enfoque más específico. En un caso, los atacantes pasaron meses dentro de la red de un objetivo recopilando cookies del navegador Microsoft Edge. Luego, los atacantes usaron una combinación de actividad de Cobalt Strike y Meterpreter para abusar de una herramienta de compilación legítima para extraer tokens de acceso.

En otro caso, los atacantes utilizaron un componente legítimo de Microsoft Visual Studio para lanzar una carga maliciosa que extrajo archivos de cookies durante una semana.

"Si bien históricamente hemos visto robos masivos de cookies, los atacantes ahora están adoptando un enfoque específico y preciso para robar dichos tokens . Debido a que gran parte del trabajo actual se desarrolla de forma remota y está basado en la web, los tipos de actividades maliciosas que los atacantes pueden llevar a cabo con las cookies de sesión robadas son realmente interminables. Pueden alterar las infraestructuras de la nube, comprometer el correo electrónico comercial, convencer a otros empleados para que descarguen malware o incluso reescribir el código de los productos. La única limitación es su propia creatividad", dijo Gallagher.

"Lo que complica las cosas es que no hay una solución fácil. Por ejemplo, los servicios pueden acortar la vida útil de las cookies, pero eso significa que los usuarios deben volver a autenticarse con más frecuencia y, dado que los atacantes recurren a aplicaciones legítimas para obtener las cookies, las empresas deben combinar la detección de malware con el análisis del comportamiento", concluye.

Para obtener más información sobre el robo de cookies de sesión y cómo los adversarios aprovechan la técnica para llevar a cabo actividades maliciosas, lea el informe completo, "Robo de cookies: el nuevo desvío del perímetro", en Sophos.com.

###

Sobre Sophos

Sophos es un líder mundial en ciberseguridad de próxima generación y protege a más de 500.000 organizaciones y millones de consumidores en más de 150 países de las ciberamenazas más avanzadas de la actualidad. Con tecnología de inteligencia de amenazas, inteligencia artificial y aprendizaje automático de SophosLabs y SophosAI, Sophos ofrece una amplia cartera de productos y servicios avanzados para proteger a los usuarios, las redes y los puntos finales contra ransomware, malware, exploits, phishing y una amplia gama de otros ciberataques. Sophos proporciona una única consola de

gestión integrada basada en la nube, Sophos Central, la pieza central de un ecosistema de ciberseguridad adaptable que cuenta con un lago de datos centralizado que aprovecha un amplio conjunto de API abiertas disponibles para clientes, socios, desarrolladores y otros proveedores de ciberseguridad. Sophos vende sus productos y servicios a través de socios revendedores y proveedores de servicios administrados (MSP) en todo el mundo. Sophos tiene su sede en Oxford, Reino Unido. Hay más información disponible en www.sophos.com

Síguenos en:
Facebook: https://www.facebook.com/SophosLatam/
Twitter: https://twitter.com/SophosLatAm
LinkedIn: https://www.linkedin.com/company/sophos/