Investigadores de seguridad cibernética advierten sobre la filtración de *«un tesoro de información confidencial»* a través de urlscan.io, un escáner de sitios web en busca de URL sospechosas y maliciosas.

> *«Las URL sensibles a documentos compartidos, páginas de restablecimiento de contraseña, invitaciones de equipo, facturas de pago y más se enumeran públicamente y se pueden buscar»,* dijo el cofundador de Positive Security, Fabian Bräunlein, en un informe publicado el 2 de noviembre de 2022.

La compañía de seguridad cibernética con sede en Berlín dijo que inició una investigación a raíz de una notificación enviada por GitHub en febrero de 2022 a un número desconocido de usuarios sobre compartir sus nombres de usuario y nombres de repositorios privados (es decir, URL de páginas de GitHub) a urlscan.io para análisis de metadatos como parte de un proceso automatizado.

Urlscan.io, que ha sido descrito como una caja de arena para la web, está integrado en varias soluciones de seguridad por medio de su API.

> *«Con el tipo de integración de esta API (por ejemplo, a través de una herramienta de seguridad que escanea todos los correos electrónicos entrantes y realiza un escaneo de URL en todos los enlaces) y la cantidad de datos en la base de datos, hay una gran variedad de datos confidenciales que pueden ser buscados y recuperados por un usuario anónimo»*, dijo Bräunlein.

Esto incluía enlaces de restablecimiento de contraseña, enlaces de cancelación de suscripción de correo electrónico, URL de creación de cuentas, claves API, información sobre bots de Telegram, solicitudes de firma de DocuSign, enlaces compartidos de Google Drive, transferencias de archivos de Dropbox, enlaces de invitación a servicios como SharePoint, Discord, Zoom, facturas de PayPal, Cisco, grabaciones de reuniones de Webex e incluso

direcciones URL para el seguimiento de paquetes.

Bräunlein dijo que una búsqueda inicial en febrero reveló *«URL jugosas»* pertenecientes a dominios de Apple, algunas de las cuales también consistían en enlaces compartidos públicamente a archivos de iCloud y respuestas de invitación de calendario. Desde entonces han sido eliminados.

Se cree que Apple solicitó la exclusión de sus dominios de los escaneos de URL, de forma que los resultados que coincidan con ciertas reglas predefinidas se eliminan de forma periódica.

Positive Security agregó también que se comunicó con varias de esas direcciones de correo electrónico filtradas y recibió una respuesta de una organización no identificada que rastreó la filtración de un enlace de contrato de trabajo de DocuSign a una configuración incorrecta de su solución de Orquestación, Automatización y Respuesta de Seguridad (SOAR), que se estaba integrando con urlscan.io.

Además de eso, el análisis también encontró que las herramientas de seguridad mal configuradas envían cualquier enlace recibido por correo como un escaneo público a urlscan.io.

Esto podría tener graves consecuencias en las que un atacante puede activar enlaces de restablecimiento de contraseña para las direcciones de correo electrónico afectadas y explotar los resultados del análisis para capturar las URL y hacerse cargo de las cuentas restableciendo la contraseña que elija el atacante.

Para maximizar la efectividad de dicho ataque, el adversario puede buscar sitios de notificación de violación de datos como Have I Been Pwned, para determinar los servicios exactos que se registraron utilizando las direcciones de correo electrónico en cuestión.

Urlscan.io, después de la divulgación responsable de Positive Security en julio de 2022, instó a los usuarios a *«comprender las diferentes visibilidades del escaneo, revisar sus propios escaneos en busca de información no pública, revisar sus flujos de trabajo de envío automatizado, y hacer cumplir una visibilidad de escaneo máxima para su cuenta».*

También agregó las reglas de eliminación para eliminar regularmente escaneos pasados y futuros que coincidan con los patrones de búsqueda, indicando que tiene listas de bloqueo de patrones de dominio y URL para evitar el escaneo de sitios web particulares.

> *«Esta información podría ser utilizada por los spammers para recopilar direcciones de correo electrónico y otra información personal. Los ciberdelincuentes podrían usarlo para apoderarse de cuentas y ejecutar campañas de phishing creíbles».*