Investigadores de seguridad cibernética describieron una técnica de phishing evasiva que los hackers están explotando en la naturaleza para atacar a los visitantes de varios sitios web con una peculiaridad en los nombres de dominio, y aprovechar los favicons modificados para inyectar e-skimmers y robar información de tarjetas bancarias de forma encubierta.

> *«La idea es simple y consiste en usar caracteres que se ven iguales para engañar a los usuarios. A veces los caracteres son de un idioma diferente o simplemente escriben en mayúscula la letra 'i' para que parezca una 'l' minúscula»,* dijeron los investigadores de Malwarebytes.

Llamada ataque homógrafo de nombre de dominio internacionalizado (IDN), la técnica ha sido utilizada por un grupo de Magecart en mútiples dominios para cargar el popular kit de skimming de Inter oculto dentro de un archivo favicon.

El truco visual generalmente implica aprovechar las similitudes de los scripts de caracteres para crear y registrar dominios fraudulentos de los existentes para engañar a los usuarios desprevenidos para que los visiten e introduzcan malware en los sistemas de destino.

En varios casos, Malwarebytes descubrió que los sitios web legítimos fueron pirateados e inyectados con un código inofensivo que hacía referencia a un archivo de icono que carga una versión copiada del favicon del sitio señuelo.

Este favicon cargado desde el dominio homoglyph se utilizó posteriormente para inyectar el skimmer de Inter JavaScript que captura la información ingresada en una página de pago y extrae los detalles al mismo dominio utilizado para alojar el archivo favicon malicioso.

Uno de los dominios falsos («zoplm.com»), que se registró el mes pasado, ha estado vinculado previamente a Magecart Group 8, uno de los grupos de hackers que se ha vinculado a ataques de skimming web en NutriBullet, MyPillow, además de varios sitios web

propiedad de una bolsa nacional de diamantes.

La violación de MyPillow, particularmente, se menciona debido a las similitudes en el modus operandi, que implicó la inyección JavaScript de terceros alojada en «mypiltow.com», un homógrafo de «mypillow.com».

> *«A los actores de amenazas les encanta aprovechas cualquier técnica que les proporcione una capa de evasión, por pequeña que sea. La reutilización del código plantea un problema para los defensores, ya que difumina las líneas entre los diferentes ataques que vemos y dificulta cualquier tipo de atribución»*, dijeron los investigadores.

Debido al aumento de casos de phishing y la sofisticación de estos, es recomendable que los usuarios revisen detenidamente los nombres de dominio y certificado de seguridad para asegurarse de que se encuentran en el sitio correcto.