Investigadores de seguridad informática han detectado múltiples operaciones dirigidas contra Docker Hub mediante la inserción de millones de contenedores maliciosos *«sin imágenes»* en los últimos cinco años, lo que destaca nuevamente la posibilidad de ataques a la cadena de suministro a través de registros de código abierto.

> Andrey Polkovnichenko, un investigador en seguridad de JFrog, compartió en un informe: *«Más de cuatro millones de los repositorios en Docker Hub carecen de imágenes y solo contienen la documentación del repositorio».*

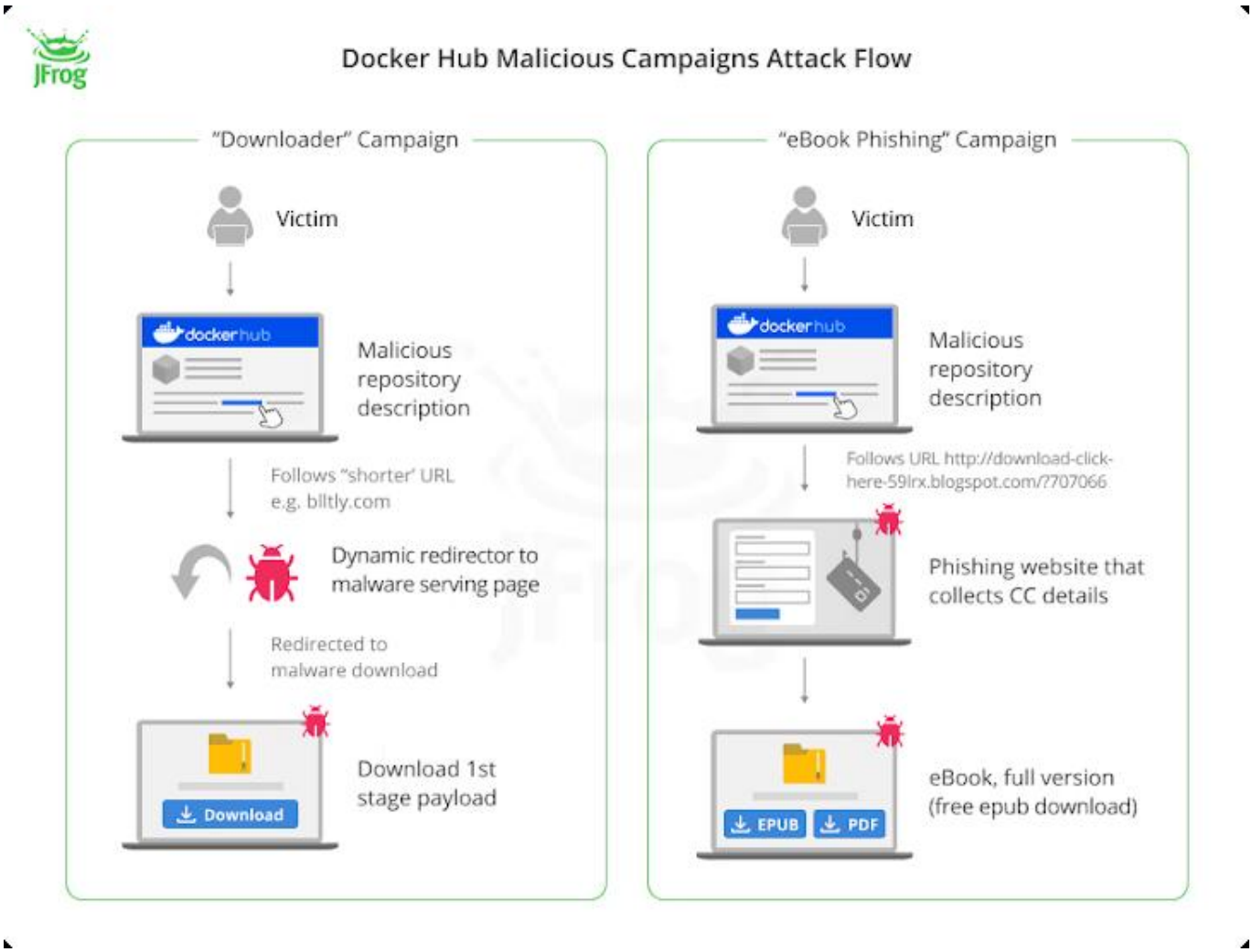
Además, la documentación no está relacionada en absoluto con el contenedor. En cambio, es una página web diseñada para atraer a los usuarios a visitar sitios de phishing o de alojamiento de malware.

De los 4.79 millones de repositorios sin imágenes descubiertos en Docker Hub, se estima que 3.2 millones de ellos se han utilizado como páginas de destino para redirigir a usuarios desprevenidos a sitios fraudulentos como parte de tres campañas amplias:

- Descargador (repositorios creados en la primera mitad de 2021 y septiembre de 2023), que promociona enlaces a contenido supuestamente pirateado o trucos para videojuegos, pero que en realidad conducen directamente a fuentes maliciosas o a una legítima que, a su vez, contiene código JavaScript que redirige a la carga maliciosa después de 500 milisegundos.
- Phishing de libros electrónicos (repositorios creados a mediados de 2021), que desvía a los usuarios que buscan libros electrónicos a un sitio web («rd.lesac.ru») que, a su vez, les insta a ingresar su información financiera para descargar el libro electrónico.
- Sitio web (miles de repositorios creados diariamente desde abril de 2021 hasta octubre de 2023), que incluye un enlace a un servicio de alojamiento de diarios en línea llamado Penzu en algunos casos.

La carga útil entregada como parte de la campaña del descargador está diseñada para conectarse a un servidor de comando y control (C2) y enviar metadatos del sistema, después

de lo cual el servidor responde con un enlace a software crackeado.



Por otro lado, el objetivo preciso del conjunto de sitios web aún no está claro, ya que la campaña también se propaga en sitios que tienen una política de moderación de contenido menos estricta.

> *«La preocupación principal de estas tres campañas radica en que los usuarios*

> *tienen escasas opciones para resguardarse desde el principio, más allá de ejercer precaución»,* comentó Shachar Menashe, director senior de investigación de seguridad en JFrog.
>
> *«Básicamente, estamos observando un campo de pruebas para malware que, en algunos casos, ha estado en desarrollo durante tres años. Estos actores de amenazas están altamente motivados y se amparan en la credibilidad del nombre de Docker Hub para atraer a las víctimas».*

Dado el esfuerzo meticuloso que los actores de amenazas invierten en envenenar utilidades ampliamente conocidas, tal como se evidencia en el caso del compromiso de XZ Utils, es fundamental que los desarrolladores procedan con cautela al descargar paquetes de los ecosistemas de código abierto.

> *«Como sugiere la Ley de Murphy, si algo puede ser explotado por desarrolladores de malware, inevitablemente lo será, por lo que esperamos que estas campañas puedan encontrarse en más repositorios además de Docker Hub»,* añadió Menashe.