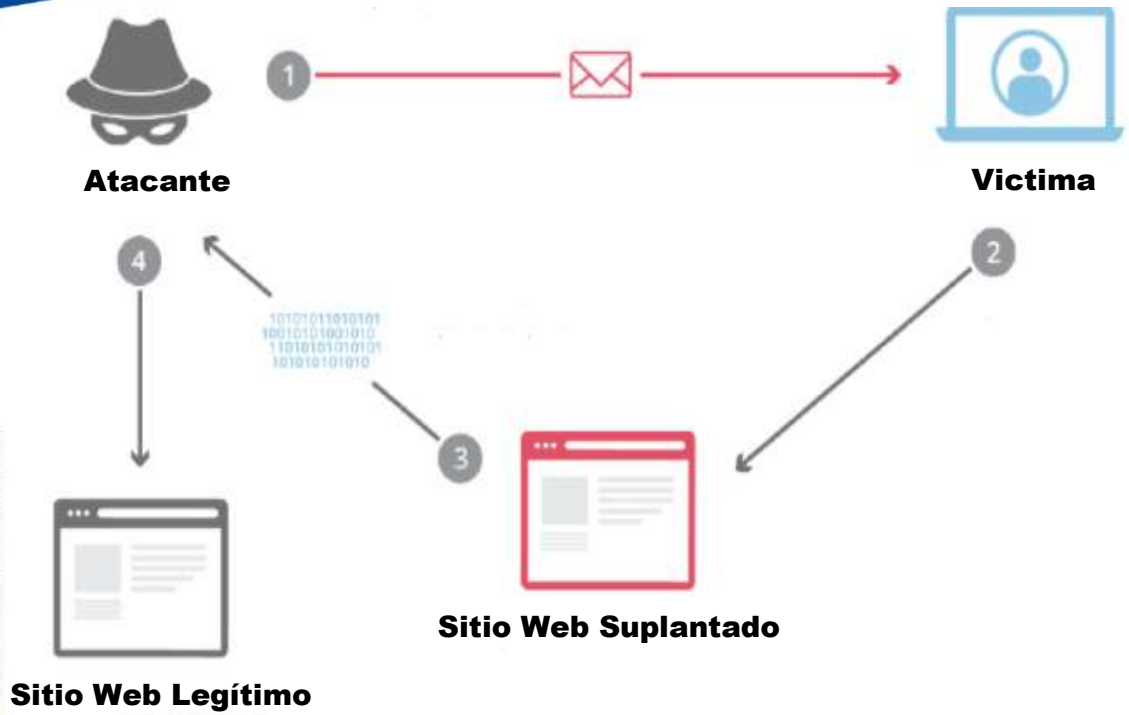
Conozca como se ejecuta un ataque Phishing



1. El atacante envía un correo electrónico a la víctima con contenido convincente o amenazante que genera interés.
2. La victima abre el correo electrónico y hace clic en un enlace (link) pensando en que lo direccionará a la página oficial del remitente, que en realidad es un sitio suplantado, también en algunos casos el usuario descarga archivos adjuntos que generalmente están en formato PDF que incluyen (extractos bancarios, multas, pagos de impuesto, comparendos, etc.) que contienen un enlace en el que el usuario hace clic y descarga e instala malware con el propósito de mantener un acceso remoto ejecutándose en el computador de la víctima.
3. El atacante recolecta las credenciales de las víctimas.
4. El atacante utiliza las credenciales de las victimas (contraseñas, tarjetas de crédito, datos financieros) para robar su identidad, su dinero, o utilización de sus cuentas para actividades delictivas.

Tomado y adaptado de: https://www.welivesecurity.com/la-es/2021/01/12/operacion-spalax-ataques-malware-dirigidos-colombia/

BOLETÍN MENSUAL DE NOTICIAS Y NOVEDADES DE SEGURIDAD INFORMÁTICA.

Temas mas comunes para ejecutar un ataque de PHISHING por correo electrónico

En la mayoría de estos correos electrónicos se hace referencia a temas genéricos que podrían reutilizarse para diferentes objetivos.

Encontramos correos electrónicos de phishing con estos temas:

- Una notificación sobre una infracción de tránsito.
- Una notificación indicando que debe realizarse una prueba de COVID-19 obligatoria.
- Una notificación para asistir a una audiencia judicial
- Una investigación abierta contra el destinatario por malversación de fondos públicos.
- Una notificación de un embargo de cuentas bancarias.

Tomado y adaptado de: https://www.welivesecurity.com/la-es/2021/01/12/operacion-spalax-ataques-malware-dirigidos-colombia/

Universidad de Santander
Personería Jur. 810 de 12/03/96 Min.Educación UDES

BOLETÍN MENSUAL DE NOTICIAS Y NOVEDADES DE SEGURIDAD INFORMÁTICA.

ALERTA DE PHISHING CIRCULANDO EN LA RED

Modalidad de phishin se presenta mediante el envío de correos electrónicos a nombre de #MiVacuna, en donde se solicita llenar un formulario de inscripción para acceder a un turno en la primera fase de vacunación. ¡No te dejes engañar! No suministre información ni agra documentos adjuntos en el mensaje. El único portal habilitado para postularse a la vacunación es http://mivacuna.sispro.gov.co

Tomado y adaptado de: https://www.minsalud.gov.co

JUICE JACKING: EL RIESGO DE LOS CARGADORES USB PÚBLICOS INTERVENIDOS

Si alguna vez ha tenido que cargar su celular en un lugar público como aeropuertos, oficinas, parques, museos, entre otros, debe saber que los cibercriminales pueden alterar con fines maliciosos la fuente de carga (puertos USB) que proporciona energía, para robar su información personal o inyectar archivos maliciosos que pueden infectar su dispositivo. Se aconseja contar con una batería portable propia y no utilizar centrales de carga públicas a menos que sea de estricta necesidad, de ser así, tenga en cuenta las siguientes recomendaciones:

- Apague el dispositivo previa conexión.
- Al conectar el cable seleccionar en nuestro dispositivo la opción “solo carga” para la conexión.
- Utilice un bloqueador de datos USB.

Tomado y adaptado de: https://www.welivesecurity.com/la-es/2021/02/03/juice-jacking-riesgo-cargadores -usb-publicos-intervenidos/