Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°193	Fecha: 21-08-2024
		Página: 4 de 9

Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	Nuevos ataques de phishing en iOS y Android		
Tipo de Ataque	Phishing	Abreviatura	Phishing
Medios de propagación	Redes sociales, SMS, correo electrónico, videos de internet, entre otros		
Código de familia	G	Código de Sub familia	G01
Clasificación temática familia	Fraude		

Descripción

1. ANTECEDENTES:

Los investigadores de ESET descubrieron un tipo poco común de campaña de phishing dirigida a usuarios de Android y iPhone. Analizaron un caso observado en la red que tenía como objetivo a clientes de un importante banco checo. Dicha campaña combina técnicas tradicionales con el uso de las tecnologías PWAs de iOS y WebAPK de Android para instalar aplicaciones maliciosas sin el consentimiento del usuario.

Esta técnica fue descubierta por primera vez por el CSIRT KNF en Polonia en julio de 2023 y, en noviembre de 2023, fue observada en Chequia por analistas de ESET que trabajan en el servicio Brand Intelligence. También se observaron dos casos de campañas móviles contra bancos fuera de Chequia: un caso dirigido al banco húngaro OTP y otro dirigido al banco georgiano TBC.

2. DETALLES:

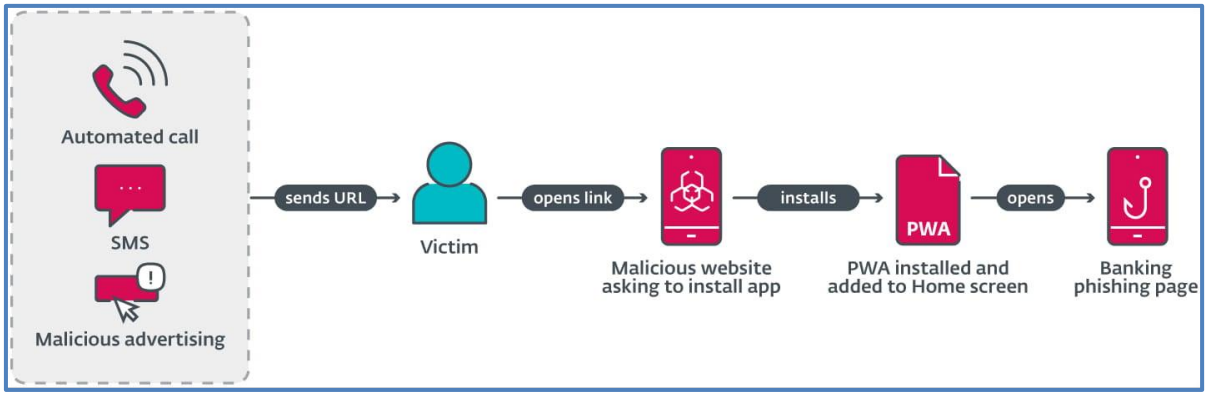
Esta técnica es notable porque instala una aplicación de phishing desde un sitio web de terceros sin que el usuario tenga que permitir la instalación de aplicaciones de terceros. En Android, esto podría dar lugar a la instalación silenciosa de un tipo especial de APK, que incluso parece instalado desde la tienda Google Play. La amenaza también iba dirigida a usuarios de iPhone (iOS).

Los sitios web de phishing dirigidos a iOS indican a las víctimas que agreguen una aplicación web progresiva (PWA) a sus pantallas de inicio, mientras que, en Android, la PWA se instala después de confirmar las ventanas emergentes personalizadas en el navegador. En este punto, en ambos sistemas operativos, estas aplicaciones de phishing son en gran medida indistinguibles de las aplicaciones bancarias reales que imitan. Las PWA son esencialmente sitios web agrupados en lo que parece una aplicación independiente, y esta sensación se mejora con el uso de mensajes nativos del sistema. Las PWA, al igual que los sitios web, son multiplataforma, lo que explica cómo estas campañas de phishing de PWA pueden dirigirse tanto a usuarios de iOS como de Android.

"Para los usuarios de iPhone, una acción de este tipo podría romper cualquier suposición de 'jardín amurallado' en materia de seguridad", afirma el investigador de ESET Jakub Osmani, quien analizó la amenaza.

Esta campaña consiste en tres mecanismos de envío de URL diferentes. Estos mecanismos incluyen llamadas de voz automatizadas, mensajes SMS y publicidad maliciosa en redes sociales. La entrega de la llamada de voz se realiza a través de una llamada automatizada que advierte al usuario sobre una aplicación bancaria desactualizada y le pide que seleccione una opción en el teclado numérico. Después de presionar el botón correcto, se envía una URL de phishing por SMS, como se informó en un tuit. La entrega inicial por SMS se realizó enviando mensajes indiscriminadamente a números de teléfono checos. El mensaje enviado incluía un enlace de phishing y un texto para inducir a las víctimas a visitar el enlace mediante ingeniería social. La campaña maliciosa se difundió a través de anuncios registrados en plataformas Meta como Instagram y Facebook. Estos anuncios incluían una llamada a la acción, como una oferta limitada para los usuarios que "descarguen una actualización a continuación".

Después de abrir la URL entregada en la primera etapa, a las víctimas de Android se les presentan dos campañas distintas: una página de phishing de alta calidad que imita la página oficial de Google Play Store de la aplicación bancaria en cuestión o un sitio web que imita esa aplicación. A partir de aquí, se les pide a las víctimas que instalen una "nueva versión" de la aplicación bancaria.



Dependiendo de la campaña, al hacer clic en el botón de instalación/actualización se inicia la instalación de una aplicación maliciosa desde el sitio web, directamente en el teléfono de la víctima, ya sea en forma de WebAPK (solo para usuarios de Android) o como PWA para usuarios de iOS y Android (si la campaña no está basada en WebAPK). Este paso crucial de instalación pasa por alto las advertencias tradicionales del navegador de "instalar aplicaciones desconocidas": este es el comportamiento predeterminado de la tecnología WebAPK de Chrome, que es abusada por los atacantes.

El proceso es un poco diferente para los usuarios de iOS, ya que una ventana emergente animada indica a las víctimas cómo agregar la PWA de phishing a su pantalla de inicio.

La ventana emergente copia el aspecto de las indicaciones nativas de iOS. Al final, ni siquiera los usuarios de iOS reciben una advertencia sobre la adición de una aplicación potencialmente dañina a su teléfono.

Después de la instalación, se solicita a las víctimas que envíen sus credenciales de banca por Internet para acceder a su cuenta a través de la nueva aplicación de banca móvil. Toda la información enviada se envía a los servidores C&C de los atacantes.

3. RECOMENDACIONES:

- Descargar software únicamente de sitios web confiables y de buena reputación. Evitar hacer clic en enlaces o anuncios sospechosos, que provengan de correos electrónicos, mensajes de texto o mensajes de redes sociales que soliciten información personal.
- Revisar con atención los permisos solicitados por cualquier aplicación antes de instalarla. Desconfiar de las extensiones que solicitan un acceso excesivo a sus datos.
- Verificar la autenticidad de los sitios web.
- Utilizar contraseñas seguras y autenticación de dos factores (2FA) para las cuentas financieras.
- Mantener el software actualizado. Actualizar periódicamente el sistema operativo, navegador y software antivirus para protegerse contra las últimas amenazas.
- Utilizar una solución antivirus confiable que pueda ayudar a detectar y bloquear software malicioso.
- Educar a los usuarios sobre las amenazas de ransomware y cómo reconocer los intentos de phishing.

Fuente de Información:	• hxxps://www.eset.com/int/about/newsroom/press-releases/research/eset-research-discovers-financial-fraud-using-novel-phishing-method-tailored-to-android-and-iphone-users/ • hxxps://www.welivesecurity.com/en/eset-research/be-careful-what-you-pwish-for-phishing-in-pwa-applications/ • hxxps://ctoperu.pe/articulo/39399/eset-research-descubre-un-fraude-financiero/ • hxxps://www.bleepingcomputer.com/news/security/hackers-steal-banking-creds-from-ios-android-users-via-pwa-apps/