Componente que reporta	**CENTRO NACIONAL DE SEGURIDAD DIGITAL**		
Nombre de la alerta	Malware Zanubis dirigido para entidades financieras del Perú		
Tipo de Ataque	Malware	Abreviatura	Malware
Medios de propagación	Red, Internet		
Código de familia	C	Código de Sub familia	C02
Clasificación temática familia	Código Malicioso		

Descripción

1. **ANTECEDENTES:**

Zanubis, apareció alrededor de agosto de 2022, dirigido a instituciones financieras y usuarios de intercambio de criptomonedas en Perú. La principal ruta de infección de Zanubis es hacerse pasar por aplicaciones legítimas de Android peruano y luego **engañar al usuario para que habilite los permisos de accesibilidad** para tomar el control total del dispositivo.

2. **DETALLES:**

Recientemente (abril 2023), el malware Zanubis se disfrazó como la aplicación oficial de Android para la Superintendencia Nacional de Aduanas y de Administración Tributaria - SUNAT.

Zanubis se ofusca con la ayuda de Obfuscapk, un ofuscador popular para archivos APK de Android, una vez que la víctima concede permisos de accesibilidad a la aplicación maliciosa, esta puede operar en segundo plano sin ser detectada. El malware utiliza WebView para cargar un sitio web legítimo de SUNAT utilizado para buscar deudas.

Cuando se ejecuta el malware en el dispositivo, toma una de dos acciones, dependiendo de su configuración, para robar la información de la víctima: por eventos de registro, teclas, o grabando la pantalla.

Tambien se presume que el malware genera una puerta trasera del teléfono infectado, para que ciberdelincuentes tomen control.

Otra característica observada, es la del evento denominado “bloqueoUpdate,”, que **pretende ser una actualización de Android, evitando así que el teléfono se use**. A medida que se ejecuta la actualización, el teléfono permanece inutilizable hasta el punto de que no se puede bloquear o desbloquear, ya que el malware monitorea esos intentos y los bloquea.

Según un análisis realizado al malware**, las aplicaciones objetivo, son las entidades financieras del Perú**.

a) Indicadores de compromiso:

TIPO	INDICADOR
Hash	054061a4f0c37b0b353580f644eac554
Hash	a518eff78ae5a529dc044ed4bbd3c360
Hash	41d72de9df70205289c9ae8f3b4f0bcb
Hash	9b00a65f117756134fdb9f6ba4cef61d
Hash	8d99c2b7cf55cac1ba0035ae265c1ac5
Hash	248b2b76b5fb6e35c2d0a8657e080759
Hash	a2c115d38b500c5dfd80d6208368ff55

Imagen del evento denominado “bloqueoUpdate”, Actualización falsa que bloquea al usuario fuera del teléfono

3. RECOMENDACIONES:

- Acceder a sitios web a través de fuentes legitimas.
- Evitar la instalación de aplicaciones desde fuentes no oficiales, no recurrir a versiones alteradas o modificadas de los aplicativos.
- Asegurarse de que el software provenga de una fuente legítima en la tienda de aplicaciones de Android, conocida como "Google Play Store".
- Hacer uso de un antivirus en el dispositivo móvil.
- Realizar el bloqueo de los indicadores de compromiso en los equipos de seguridad disponibles.
- Configurar notificaciones y avisos en tus cuentas bancarias para estar al tanto de cualquier actividad sospechosa y poder tomar medidas de inmediato, incluyendo el bloqueo de las cuentas si es necesario.

Fuente de Información:	• https://www.kaspersky.com/about/press-releases/2023_unmasking-zanubis-banking-trojans-sneaky-evolution-and-cryptocurrency-threats-unveiled