MALWARE ZANUBIS

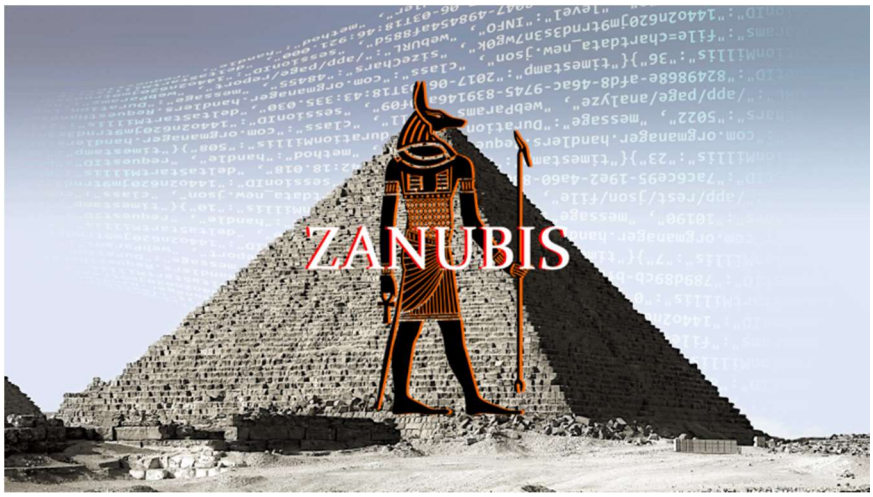

Figura 1.-Ilustración relacionada a Zanubis
Fuente: https://cuarteldelmetal.com/noticias/2023/10/zanubis-un-troyano-que-amenaza-la-seguridad-bancaria-en-android/

I. DEFINICIÓN

Zanubis es un malware del tipo troyano de origen peruano que viola los sellos de seguridad de los dispositivos móviles para robar credenciales de acceso y secuestra mensajes SMS que las instituciones bancarias envían a las víctimas, de esta manera los ciberdelincuentes pueden robar el dinero que los usuarios guardan en su banca móvil.

II. VECTORES DE ATAQUE

Zanubis se caracteriza por su especialización y enfoque en aplicaciones bancarias e instituciones financieras locales. El malware opera de la siguiente manera:

- **Robo de Credenciales:** Hurto de credenciales de acceso a cuentas bancarias y financieras.
- **Interceptación de SMS:** Zanubis es capaz de secuestrar mensajes de texto, especialmente aquellos que contienen códigos de verificación o activación enviados por entidades financieras.

Zanubis inicia su infección cuando los usuarios descargan aplicaciones malintencionadas de fuentes no oficiales. Engaña a sus víctimas disfrazando aplicaciones legales como de la Superintendencia Nacional de Aduanas y de Administración Tributaria (SUNAT).

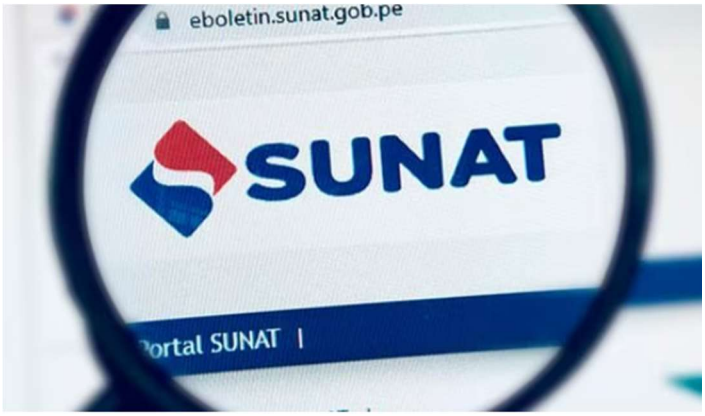

Figura 2.-Ilustración relacionada a SUNAT
Fuente: https://elcomercio.pe/respuestas/como/sunat-como-saber-el-estado-de-mi-ruc-tramites-tdpe-noticia/

Además, este troyano tiene la capacidad de manipular aplicaciones en el dispositivo infectado mediante comandos remotos y bloquear el uso del teléfono a través de actualizaciones de Android falsas, lo que coacciona a las víctimas a usar el desbloqueo biométrico, además se destaca por mostrar una página web de SUNAT que parece ser legítima para reducir las sospechas de las víctimas.

El malware verificará si la aplicación falsa se instaló por primera vez en el dispositivo y si tiene el Menú de Accesibilidad después de que el usuario ya la haya instalado, el troyano Zanubis puede mostrar alertas como "es necesario actualizar la aplicación" si el dispositivo no tiene dicho menú. Gracias a esto, puede usar "la mano fantasma".

El cibercriminal puede reducir el brillo de la pantalla del teléfono durante un ataque de mano fantasma y continuar operando sin que las víctimas se den cuenta de que están abriendo y cerrando aplicaciones. Los usuarios normalmente usan la huella dactilar para desbloquear el equipo.

Según el análisis de Kaspersky, Zanubis se comunica fluidamente en español y posee un amplio conocimiento de la jerga y las oraciones frecuentes usadas, con una gran relación con las instituciones financieras peruanas y hasta el momento, solo ha demostrado interés en estas aplicaciones.

En este momento, no se tiene conocimiento de si el troyano se distribuirá a otros países de la zona, sin embargo, es innegable que poseen un gran potencial.

En Perú, esta amenaza ya representa el 45% de los troyanos bancarios bloqueados de la lista de aplicaciones a las que el malware apunta para cometer fraudes. Según él, los troyanos brasileños representan alrededor del 25% de los intentos de infección que bloqueamos en el país.

III. MEDIDAS PARA EVITAR SER VÍCTIMA DEL MALWARE ZANUBIS

1) **Fuentes Confiables:** Solo utilice fuentes confiables y tiendas oficiales para descargar aplicaciones.
2) **Verifique los permisos:** Es fundamental revisar los permisos que solicita una aplicación para asegurarse de que sean consistentes con la funcionalidad de la aplicación.
3) **Usar Software de Seguridad:** Instalar soluciones de seguridad confiables que protegen contra el malware y sus acciones maliciosas.
4) **Evite hacer clic en enlaces desconocidos:** Si no se confirma la fuente, no haga clic en enlaces en correos electrónicos, mensajes de SMS o redes sociales.
5) **Evitar el rooting**: No rootear los dispositivos, ya que esto puede dar a los ciberdelincuentes más oportunidades para infiltrarse en los sistemas.

IV. QUE HACER ANTE UN ATAQUE DE MALWARE ZANUBIS:

1) **Desconecta de la red:** Si sospechas que tu dispositivo está infectado con malware, desconéctalo de la red de inmediato. Esto ayudará a prevenir la propagación del malware y evitará que los atacantes obtengan tus datos.
2) **Escanear al dispositivo:** Utiliza un software antivirus o antimalware actualizado para escanear su dispositivo en busca de amenazas. Asegúrate de que el software esté actualizado para que pueda identificar las amenazas más recientes.

3) **Elimina el malware**: Siga las instrucciones del software de seguridad para eliminar el malware que haya sido detectado. En ocasiones, puede ser necesario formatear y reinstalar el sistema operativo desde cero para garantizar que el malware se haya eliminado por completo.

4) **Restaure desde una copia de seguridad:** Si tiene copias de seguridad de sus datos, use una copia de seguridad limpia y verificada para restaurar sus archivos y sistemas. Asegúrate de que la copia de seguridad no contenga malware.

V. REFERENCIAS:

- CUARTELMETAL. (10 de octubre de 2023). Obtenido de https://cuarteldelmetal.com/noticias/2023/10/zanubis-un-troyano-que-amenaza-la-seguridad-bancaria-en-android/

- MARCA. (14 de octubre de 2023). Obtenido de https://www.marca.com/mx/tecnologia/2023/10/14/652afad322601d14148b45dc.html

- DEPOR. (16 de octubre de 2023). Obtenido de https://depor.com/depor-play/tecnologia/que-es-zanubis-el-troyano-que-amenaza-tus-cuentas-bancarias-en-android-y-como-evitar-la-infeccion-mexico-espana-mx-sunat-rat-kaspersky-noticia/

- INFOBAE. (03 de octubre de 2023). Obtenido de https://www.infobae.com/peru/2023/10/03/zanubis-el-virus-troyano-bancario-peruano-que-puede-vaciar-cuentas-atacando-cuentas-de-whatsapp-y-gmail/

- CIBERPRISMA. (12 de octubre de 2023). Obtenido de https://ciberprisma.org/2023/10/12/malware-zanubis-recargado-ataca-a-la-banca-movil-en-peru/