Un nuevo troyano fue descubierto atacando de forma selectiva objetivos en el Medio Oriente, al verificar los diseños del teclado e intentar evitar las listas negras abusando de los servicios en la nube.

El jueves pasado, investigadores de seguridad cibernética de Cisco Talos, dijeron que el troyano de acceso remoto (RAT), denominado JhoneRAT, se está propagando activamente por medio de documentos de Microsoft Office que contienen macros maliciosas.

El primero de los documentos identificados por medio de campañas de phishing, llamado «Urgent.docx», pide al destinatario habilitar la edición de imágenes en inglés y árabe. El segundo, «fb.docx», afirma contener datos sobre una fuga de información en Facebook, y el tercero pretende ser de una organización legítima en Emiratos Árabes Unidos.

Para todos los casos, si se habilita la edición, se carga y ejecuta un documento adicional de Office que contiene una macro maliciosa. Estos documentos se alojan por medio de Google Drive *«para evitar las listas negras de URL»*, según los investigadores.

JhoneRAT está desarrollado en Python y se elimina a través de Google Drive, que aloja imágenes con un binario codificado en base64 agregado al final. Estas imágenes, una vez cargadas en una máquina objetivo, desplegarán el troyano, que inmediatamente comenzará a recopilar información de la computadora, incluyendo el tipo, números de serie del disco duro, el sistema operativo, entre otros.

Al comunicarse con su servidor de comando y control para extraer la información, los comandos se verifican por medio de un feed público de Twitter cada 10 segundos. El identificador @jhone87438316 se usó originalmente, pero la cuenta ahora está suspendida.

> *«Estos comandos se pueden emitir a una víctima específica en función del UID generado en cada objetivo mediante el uso de información serial y contextual del disco, como el nombre del host, antivirus y el sistema operativo, o para todos ellos»,* dicen los investigadores.

Sin embargo, el robo real de datos se hace por medio de los proveedores en la nube ImgBB, Google Drive y Forms. Las capturas de pantalla se cargan en ImgBB, los binarios se descargan de Drive y los comandos se ejecutan con la salida enviada a los formularios.

Algo interesante del malware, es cómo se seleccionan los objetivos. El filtrado se implementó en función del diseño del teclado de la víctima, y el malware solo se ejecutará contra aquellos países de habla árabe.

Cisco Talos informa que JhoneRAT apunta a Arabia Saudita, Irak, Egipto, Libia, Argelia, Marruecos, Túnez, Omán, Yemen, Siria, Emiratos Árabes Unidos, Kuwuait, Bahrein y Líbano.

> *«Esta campaña comenzó en noviembre de 2019 y aún sigue. En este momento, se revoca la clave API y se suspende la cuenta de Twitter. Sin embargo, el atacante puede crear fácilmente nuevas cuentas y actualizar los archivos maliciosos para seguir funcionando»,* agregan los investigadores.

Otro troyano inusual en revisión por investigadores de amenazas actualmente, es Faketoken. Este troyano comenzó sus acciones como una forma de malware atornillado utilizado por los troyanos de escritorio tradicionales para interceptar códigos de verificación enviados a dispositivos móviles cuando las víctimas intentaron iniciar sesión en cuentas en línea y desde entonces, se ha convertido en una amenaza financiera independiente-

Recientemente, una campaña de Faketoken demostró un comportamiento extraño: el secuestro de las instalaciones de mensajería de dispositivos móviles para enviar mensajes de texto ofensivos.

Los investigadores de seguridad cibernética no saben por qué, con la excepción de que muchos destinatarios están en el extranjero, y por lo tanto, los mensajes SMS podrían generar ingresos por medio de los costosos mensajes que se envían a estos números.