Se descubrió que los hackers con presuntos vínculos con Irán aprovechan las aplicaciones de mensajería instantánea y VPN como Telegram y Pshiphon, con el fin de instalar un troyano de acceso remoto de Windows (RAT), capaz de robar información confidencial de los dispositivos de los objetivos desde al menos 2015.

La compañía rusa de seguridad cibernética Kaspersky, que reconstruyó la actividad, atribuyó la campaña a un grupo de amenazas persistentes avanzadas (APT) al que rastrea como Ferocious Kitten, un grupo que ha señalado a personas de habla persa supuestamente radicadas en el país mientras opera con éxito bajo el radar.

> *«La focalización de Psiphon y Telegram, ambos servicios muy populares en Irán, subraya el hecho de que las cargas útiles fueron desarrolladas con el fin de orientar a los usuarios iraníes en mente»,* dijeron Global Research de Kaspersky y el Equipo de Análisis.
>
> *«Además, el contenido señuelo mostrado por los archivos maliciosos por lo general utilizaba temas políticos e incluía imágenes o videos de bases de la resistencia o ataques contra el régimen iraní, lo que sugiere que el ataque está dirigido a posibles partidarios de tales movimientos dentro del país»,* agregaron.

Los hallazgos de Kaspersky surgen de dos documentos armados que se cargaron en VirusTotal en julio de 2020 y marzo de 2021, que están integrados con macros, que al ser habilitadas, eliminan las cargas útiles de la siguiente etapa para implementar un nuevo implante denominado MarkiRat.

La puerta trasera permite a los atacantes un amplio acceso a los datos personales de la víctima, que incluye funciones para registrar pulsaciones de teclas, capturar contenido del portapapeles, descargar y cargar archivos, así como la capacidad de ejecutar comandos arbitrarios en la máquina de la víctima.

En lo que parece ser un intento de expandir su arsenal, los atacantes también experimentaron con distintas variantes de MarkiRat que se encontraron para interceptar la ejecución de aplicaciones como Google Chrome y Telegram para lanzar el malware y mantenerlo anclado persistentemente a la computadora al mismo tiempo.

El tiempo también hace que sea mucho más difícil de detectar o eliminar. Uno de los artefactos descubiertos también incluye una versión trasera de Psiphon, una herramienta VPN de código abierto que se utiliza por lo general para evadir la censura de Internet.

Otra variante reciente involucra un descargador simple que recupera un ejecutable de un dominio codificado, y los investigadores señalan que *«el uso de esta muestra difiere de los utilizados por el grupo en el pasado, donde la carga útil fue eliminada por el propio malware, lo que sugiere que el grupo podría estar en proceso de cambiar algunas de sus TTP».*

Además, también se cree que la infraestructura de comando y control aloja aplicaciones de Android en forma de archivos DEX y APK, lo que aumenta la posibilidad de que los atacantes también se encuentren desarrollando de forma simultánea malware dirigido a usuarios móviles.

Las tácticas adoptadas por los atacantes se superponen con otros grupos que operan contra objetivos similares, como Domestic Kitten y Rampant Kitten, con Kaspersky encontrando paralelos en la forma en que el actor usó el mismo conjunto de servidores C2 durante largos períodos de tiempo e intentó recopilar información del administrador de contraseñas KeePass.

> *«Ferocious Kitten es un ejemplo de un actor que opera en un ecosistema más amplio destinado a rastrear individuos en Irán. Estos grupos de amenazas no parecen estar cubiertos con tanta frecuencia, por lo tanto, pueden salirse con la suya reutilizando casualmente la infraestructura y los conjuntos de herramientas sin*

> *preocuparse de que sean eliminados o marcados por las soluciones de seguridad»*, dijeron los investigadores.