Las organizaciones en naciones de habla hispana de México y España, están en el punto de mira de una nueva campaña diseñada para entregar el troyano bancario Grandoreiro.

> *«En esta campaña, los atacantes se hacen pasar por funcionarios gubernamentales de la Procuraduría General de Justicia de la Ciudad de México y del Ministerio Público en forma de correos electrónicos de spear-phishing, con el fin de atraer a las víctimas para que descarguen y ejecuten 'Grandoreiro', un prolífico troyano bancario que ha estado activo desde al menos 2016, y apunta específicamente a usuarios en América Latina»,* dijo Zscaler en un informe.

Se ha observado que los ataques en curso, que comenzaron en junio de 2022, se dirigen a los sectores de la construcción automotriz, civil e industrial, la logística y la maquinaria por medio de múltiples cadenas de infección en México y las industrias de fabricación de productos químicos en España.

Las cadenas de ataque implican aprovechar los correos electrónicos de spear-phishing escritos en español para engañar a las víctimas potenciales para que hagan clic en un enlace incrustado que recupera un archivo ZIP, del cual se extrae un cargador que se hace pasar por un documento PDF para desencadenar la ejecución.

Los mensajes de phishing incorporan de forma destacada temas que giran en torno a reembolsos de pagos, notificaciones de litigios, cancelación de préstamos hipotecarios y comprobantes de depósito, para activar las infecciones.

> *«Este cargador es responsable de descargar, extraer y ejecutar la carga útil final de 400 MB de Grandoreiro desde un servidor HFS remoto que se comunica con el servidor usando un tráfico idéntico al de LatentBot»,* dijo Nirak Shivtarkar, investigador de Zscaler.

Además, el cargador también está diseñado para recopilar información del sistema, recuperar una lista de soluciones antivirus instaladas, billeteras de criptomonedas, aplicaciones bancarias y de correo y filtrar la información a un servidor remoto de comando y control.

Observado en la naturaleza durante al menos seis años, Grandoreiro es una puerta trasera modular con una variedad de funcionalidades que le permiten registrar pulsaciones de teclas, ejecutar comandos arbitrarios, imitar los movimientos del mouse y teclado, restringir el acceso a sitios web específicos, actualizarse automáticamente y establecer persistencia por medio de un cambio en el Registro de Windows.

El malware está escrito en Delphi y utiliza técnicas como relleno binario para inflar el tamaño binario en 200 MB, implementación de CAPTCHA para evasión de sandbox y comunicación C2 usando subdominios generados a través de un algoritmo de generación de dominio (DGA).

La técnica CAPTCHA, particularmente, requiere la finalización manual de la prueba de desafío-respuesta para ejecutar el malware en la máquina comprometida, lo que significa que el implante no se ejecuta a menos y hasta que la víctima resuelva el CAPTCHA.

Los hallazgos sugieren que Grandoreiro está evolucionando continuamente hacia un malware sofisticado con características novedosas de antianálisis, otorgando a los hackers capacidades de acceso remoto total y representando amenazas significativas para los empleados y sus organizaciones.

El desarrollo llega un poco más de un año después de que las autoridades españolas detuvieran a 16 personas pertenecientes a una red criminal en relación con la operación Mekotio y Grandoreiro en julio de 2021.