Fuente:
Tynmagazine

Check Point Research (CPR), la división de Inteligencia de Amenazas de Check Point Software Technologies Ltd., un proveedor líder especializado en ciberseguridad a nivel mundial, alerta de que después de que la Guardia Civil española haya detenido a 16 sospechosos acusados de blanqueo de capitales, el troyano bancario utilizado en esos delitos vuelve a aparecer. Con el nombre de Mekotio, este malware se dirige a las víctimas de América Latina con nuevas capacidades y técnicas de evasión. En las últimas semanas, se han detectado y bloqueado más de 100 ciberataques dirigidos a países latinoamericanos que aprovechan una forma evolucionada de un troyano bancario llamado Mekotio.

Mekotio, un troyano bancario modular que tenía como objetivo los países de América Latina procedente de Brasil, ha vuelto a aparecer recientemente con un nuevo flujo de infección. La nueva campaña comenzó justo después de que la Guardia Civil española anunciara la detención de 16 personas implicadas en la distribución de Mekotio en julio de 2021. Parece que la banda detrás del malware fue capaz de reducir la brecha rápidamente y cambiar de táctica para evitar la detección.

Se cree que la cepa de malware Mekotio es obra de grupos de ciberdelincuentes brasileños que se encargan de alquilar el acceso a sus herramientas a otras bandas responsables de distribuir el troyano y blanquear fondos. Desarrollado para atacar equipos Windows, Mekotio es conocido por utilizar correos electrónicos falsos que imitan a empresas legítimas. Una vez infectada la víctima, el troyano bancario permanece oculto, esperando a que los usuarios se conecten a las cuentas bancarias electrónicas, recogiendo silenciosamente sus credenciales.

Las recientes observaciones de Check Point Research revela que estos ciberdelincuentes siguen activos, distribuyendo una nueva versión de este troyano con nuevas y mejoradas capacidades de ocultación y técnicas de evasión. España, Brasil, Chile, México y Perú han sido históricamente los objetivos de Mekotio, incluyendo los recientes ciberdelincuentes captados por los investigadores.

Cómo funciona la nueva versión de Mekotio

La infección comienza y se distribuye con un correo electrónico de phishing, escrito en español, que contiene un enlace a un archivo zip o un archivo comprimido como adjunto. El mensaje atrae a la víctima para que descargue y extraiga este contenido. Los emails captados por los investigadores reclaman a la víctima objetivo un «recibo fiscal digital pendiente de presentación». Cuando las víctimas hacen clic en el

enlace, se descarga un archivo zip fraudulento desde un sitio web malicioso. El nuevo vector de infección de Mekotio contiene estos elementos inéditos:

- Un archivo batch más sigiloso con al menos dos capas de ofuscación.
- Un nuevo script PowerShell sin archivos que se ejecuta directamente en la memoria.
- Uso de Themida v3 para empaquetar la carga útil DLL final.

En los últimos 3 meses, se han visto aproximadamente 100 ataques que utilizan nuevas y sencillas técnicas de ofuscación, con la ayuda de un cifrado de sustitución, para ocultar el primer módulo del ataque. Esta sencilla técnica de ocultación que permite que no sea detectado por la mayoría de los softwares de protección.

Correo electrónico de phishing

El email de phishing, redactado en español, afirma que hay un recibo fiscal digital pendiente de presentación. Cuando las víctimas hacen clic en el enlace del correo electrónico, se descarga un archivo zip malicioso desde un website malicioso.

Nuevas habilidades de camuflaje y técnicas de evasión

Una de las características clave de Mekotio es su diseño modular, que da a los ciberdelincuentes la posibilidad de cambiar sólo una pequeña parte del conjunto para evitar su detección. Además, Mekotio utiliza un antiguo método llamado «cifrado de sustitución» para ocultar el contenido de los archivos y el primer módulo de ataque. Esta sencilla técnica de evita ser detectado por la mayoría de los productos antivirus. Además, estos ciberdelincuentes utilizan una nueva versión de una herramienta comercial llamada «Themida», que incorpora a la descarga útil un sofisticado sistema de cifrado, antidepuración y antimonitorización.

Cómo mantenerse protegido

1. Tener cuidado con los dominios parecidos, con los errores ortográficos en los correos electrónicos o en las páginas web y con los remitentes de emails desconocidos.

2. Es preciso ser precavido con los archivos recibidos por correo electrónico de personas extrañas, sobre todo si solicitan una acción determinada que no se suele realizar.

3. Asegurarse de que los pedidos se realizan a una fuente auténtica. Una forma de hacerlo es no hacer clic en los enlaces promocionales de los mensajes y, en su lugar, buscar en Google la tienda deseada y hacer clic en el enlace de la página de resultados.

4. Hay que tener cuidado con las ofertas «especiales» que no parecen ser oportunidades de compra fiables o de confianza.

5. Garantizar que no se reutilizan las contraseñas entre diferentes aplicaciones y cuentas.

Disponible en:
https://tynmagazine.com/troyano-bancario-dirigido-a-america-latina-vuelv... [1]

Links
[1] https://tynmagazine.com/troyano-bancario-dirigido-a-america-latina-vuelve-con-fuerza/