Un grupo de hacktivistas conocido como Head Mare ha sido relacionado con ciberataques dirigidos exclusivamente a organizaciones en Rusia y Bielorrusia.

> *«Head Mare emplea métodos más avanzados para obtener acceso inicial,»* indicó Kaspersky en un análisis realizado el lunes sobre las tácticas y herramientas del grupo.
>
> *«Por ejemplo, los atacantes aprovecharon la vulnerabilidad CVE-2023-38831 en WinRAR, relativamente reciente, que permite ejecutar código arbitrario en el sistema mediante un archivo preparado de manera especial. Este método permite al grupo distribuir y ocultar la carga maliciosa de manera más eficaz.»*

Head Mare, activo desde 2023, es uno de los grupos de hacktivistas que ataca a organizaciones rusas en el contexto del conflicto ruso-ucraniano que comenzó un año antes.

El grupo también mantiene una presencia en X, donde ha filtrado información confidencial y documentos internos de sus víctimas. Los objetivos de sus ataques incluyen sectores como el gubernamental, transporte, energía, manufactura y medio ambiente.

A diferencia de otros grupos hacktivistas que parecen actuar con el objetivo de causar *«el mayor daño posible»* a las empresas en ambos países, Head Mare también cifra los dispositivos de las víctimas usando LockBit para Windows y Babuk para Linux (ESXi), exigiendo un rescate para la desencriptación de los datos.

Su conjunto de herramientas incluye PhantomDL y PhantomCore, siendo el primero un backdoor basado en Go, capaz de entregar cargas adicionales y subir archivos relevantes a un servidor de comando y control (C2).

PhantomCore (también conocido como PhantomRAT), predecesor de PhantomDL, es un troyano de acceso remoto con funciones similares, que permite descargar archivos del

servidor C2, subir archivos desde un host comprometido al servidor C2, y ejecutar comandos en el intérprete de línea de comandos cmd.exe.

> *«Los atacantes crean tareas programadas y valores en el registro llamados MicrosoftUpdateCore y MicrosoftUpdateCoree para camuflar su actividad como si estuviera relacionada con el software de Microsoft,»* señaló Kaspersky.
>
> *«También descubrimos que algunas muestras de LockBit usadas por el grupo tenían los siguientes nombres: OneDrive.exe [y] VLC.exe. Estas muestras estaban ubicadas en el directorio C:\ProgramData, disfrazadas como aplicaciones legítimas de OneDrive y VLC.»*

Se ha comprobado que estos archivos se distribuyen mediante campañas de phishing que utilizan documentos de negocios con doble extensión (por ejemplo, решение №201-5_10вэ_001-24 к пив экран-сои-2.pdf.exe о тз на разработку.pdf.exe).

Otro componente esencial de su arsenal de ataque es Sliver, un marco C2 de código abierto, junto con una colección de herramientas de acceso público como rsockstun, ngrok, y Mimikatz que facilitan la detección, el movimiento lateral y la recopilación de credenciales.

Las intrusiones culminan con el despliegue de LockBit o Babuk dependiendo del entorno objetivo, seguido por la aparición de una nota de rescate que solicita un pago a cambio de un descifrador para recuperar los archivos.

> *«Las tácticas, métodos, procedimientos y herramientas empleadas por el grupo Head Mare son en general similares a las de otros grupos que atacan organizaciones en Rusia y Bielorrusia en el contexto del conflicto ruso-ucraniano,»* señaló el proveedor ruso de ciberseguridad.

> *«Sin embargo, el grupo se diferencia por utilizar malware desarrollado a medida como PhantomDL y PhantomCore, además de explotar una vulnerabilidad relativamente nueva, CVE-2023-38831, para infiltrarse en la infraestructura de sus víctimas a través de campañas de phishing.»*