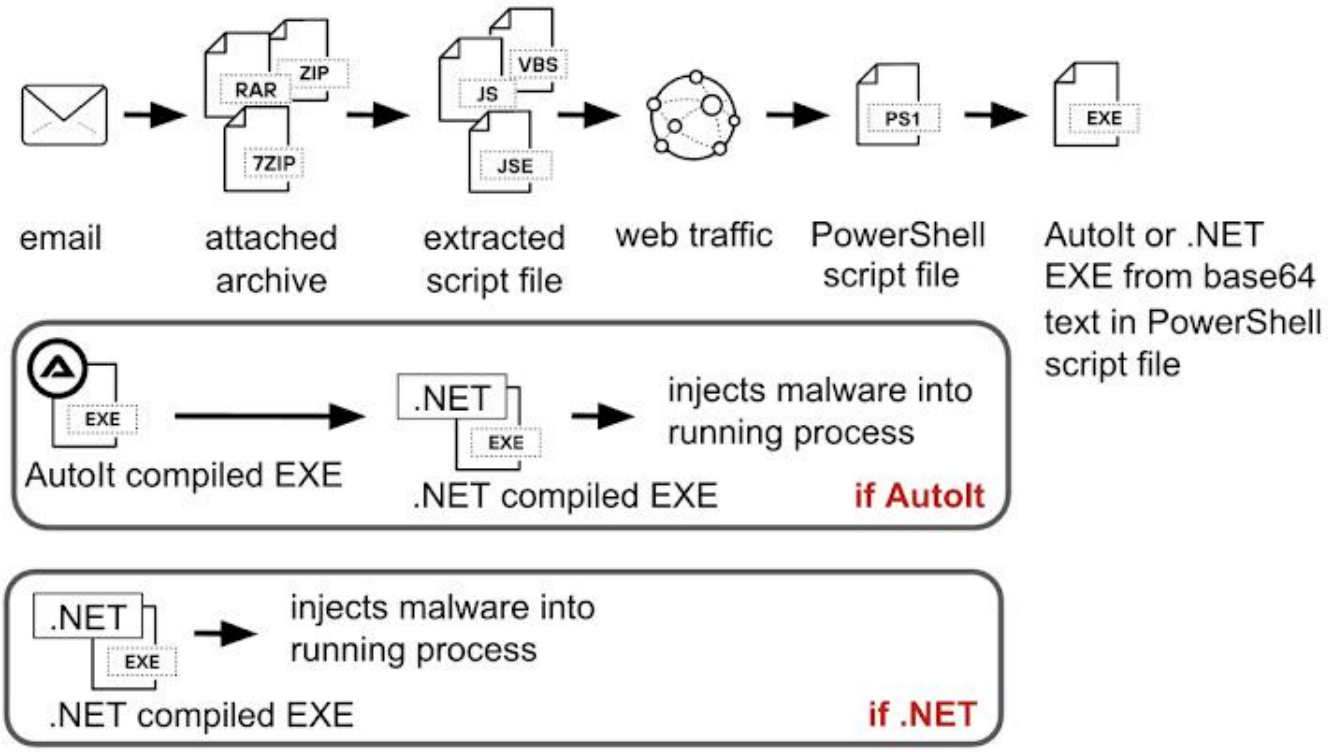
Se ha detectado una nueva campaña de ciberataques compuesta por varias etapas que distribuye diferentes tipos de malware, incluyendo variantes de Agent Tesla, Remcos RAT y XLoader.

Según el investigador Saqib Khanzada de Unit 42 de Palo Alto Networks, *«los atacantes cada vez dependen más de mecanismos de entrega complejos para evadir la detección, eludir entornos de análisis tradicionales y asegurar que el malware se entregue y ejecute con éxito».*

El ataque comienza con un correo electrónico engañoso que simula ser una solicitud de pedido. Este mensaje incluye un archivo comprimido en 7-Zip que contiene un archivo JavaScript codificado (.JSE).

Este correo, observado en diciembre de 2024, afirmaba falsamente que se había realizado un pago e instaba al destinatario a revisar el archivo adjunto. Al ejecutar el archivo JavaScript, se inicia la cadena de infección, descargando un script PowerShell desde un servidor externo.

Ese script contiene una carga útil codificada en Base64 que, una vez descifrada, se guarda en el directorio temporal de Windows y se ejecuta. En este punto, entra en juego un segundo archivo malicioso, conocido como dropper, que puede estar compilado en .NET o AutoIt.



- En el caso del ejecutable .NET, se decodifica y se inyecta una carga cifrada —una variante de Agent Tesla, posiblemente Snake Keylogger o XLoader— en un proceso activo llamado RegAsm.exe, una técnica ya utilizada en campañas anteriores de Agent Tesla.
- En el caso del ejecutable AutoIt, se añade una capa adicional que dificulta el análisis. Este script AutoIt incluye una carga encriptada que carga el código final (shellcode), haciendo que el archivo .NET sea inyectado en RegSvcs.exe, lo que finalmente activa Agent Tesla.

> Khanzada comentó: *«Esto sugiere que los atacantes utilizan múltiples rutas de ejecución para aumentar la resiliencia y evitar la detección. Su enfoque está en una cadena de ataque con varias capas más que en técnicas de ofuscación sofisticadas».*

> *«Al usar varias etapas simples en lugar de técnicas muy complejas, los atacantes pueden crear cadenas resistentes que dificultan el análisis y la detección.»*

IronHusky Lanza Nueva Versión del Troyano MysterySnail RAT

Por otro lado, la empresa Kaspersky reportó una campaña dirigida a organismos gubernamentales en Mongolia y Rusia, que utiliza una nueva versión del troyano MysterySnail RAT. Esta actividad ha sido atribuida a un grupo de habla china conocido como IronHusky, activo desde al menos 2017.

Anteriormente, este grupo fue vinculado a la explotación del CVE-2021-40449, una vulnerabilidad en Win32k que permite elevar privilegios y desplegar MysterySnail, según informó Kaspersky en 2021.

El ataque parte de un script malicioso para Microsoft Management Console (MMC) que finge ser un documento de Word de la Agencia Nacional de Tierras de Mongolia. Este script descarga un archivo ZIP que contiene un documento señuelo, un binario legítimo llamado CiscoCollabHost.exe, y una DLL maliciosa CiscoSparkLauncher.dll.

Aunque no está claro cómo se distribuye este script a los objetivos, se sospecha que se hace mediante phishing.

Al igual que en muchos ataques, CiscoCollabHost.exe es utilizado para cargar la DLL maliciosa (técnica conocida como sideloading), que actúa como una puerta trasera capaz de comunicarse con servidores controlados por los atacantes mediante el uso del proyecto piping-server de código abierto.

Esta puerta trasera puede ejecutar comandos, subir y bajar archivos, listar carpetas, borrar archivos, crear procesos nuevos o cerrarlos. Todo esto sirve para finalmente desplegar el MysterySnail RAT.

La versión más reciente del malware puede aceptar hasta 40 comandos diferentes,

permitiéndole administrar archivos, ejecutar comandos mediante cmd.exe, manipular procesos, servicios y conectarse a recursos de red mediante módulos DLL especializados.

Después de que las organizaciones atacadas tomaran medidas para bloquear las intrusiones, los atacantes comenzaron a distribuir una versión más ligera y adaptada del malware, apodada MysteryMonoSnail.

> *«Esta versión no tiene tantas funciones como el MysterySnail original. Solo incluye 13 comandos básicos, como listar archivos, escribir datos o lanzar procesos y shells remotos», explicó Kaspersky.*