El Grupo Lazarus, un infame actor de amenazas vinculado a la República Popular Democrática de Corea (RPDC), ha sido observado utilizando una *«cadena de infección compleja»* dirigida a al menos dos empleados de una organización no identificada relacionada con la energía nuclear durante el mes de enero de 2024.

Los ataques culminaron con la implementación de un nuevo backdoor modular denominado CookiePlus y forman parte de una campaña de ciberespionaje de larga duración conocida como Operación Dream Job, también rastreada como NukeSped por la empresa de ciberseguridad Kaspersky. Esta campaña ha estado activa desde al menos 2020, cuando fue expuesta por ClearSky.

Estas actividades suelen involucrar el ataque a desarrolladores y empleados de diversas empresas, incluidos sectores como defensa, aeroespacial, criptomonedas y otros sectores globales, utilizando atractivas ofertas de empleo que finalmente conducen a la instalación de malware en sus dispositivos.

> *«Lazarus está interesado en llevar a cabo ataques a la cadena de suministro como parte de la campaña DeathNote, pero esto generalmente se limita a dos métodos: el primero consiste en enviar un documento malicioso o un visor de PDF troyanizado que muestra descripciones de trabajo personalizadas al objetivo»*, señaló la empresa rusa en un análisis exhaustivo.
>
> *«El segundo método implica la distribución de herramientas de acceso remoto troyanizadas, como VNC o PuTTY, para convencer a los objetivos de conectarse a un servidor específico para una evaluación de habilidades.»*

El conjunto más reciente de ataques documentado por Kaspersky emplea el segundo método, en el que los atacantes utilizaron una cadena de infección completamente renovada que entrega una utilidad VNC troyanizada bajo el pretexto de realizar una evaluación de habilidades para puestos de TI en destacadas empresas aeroespaciales y de defensa.

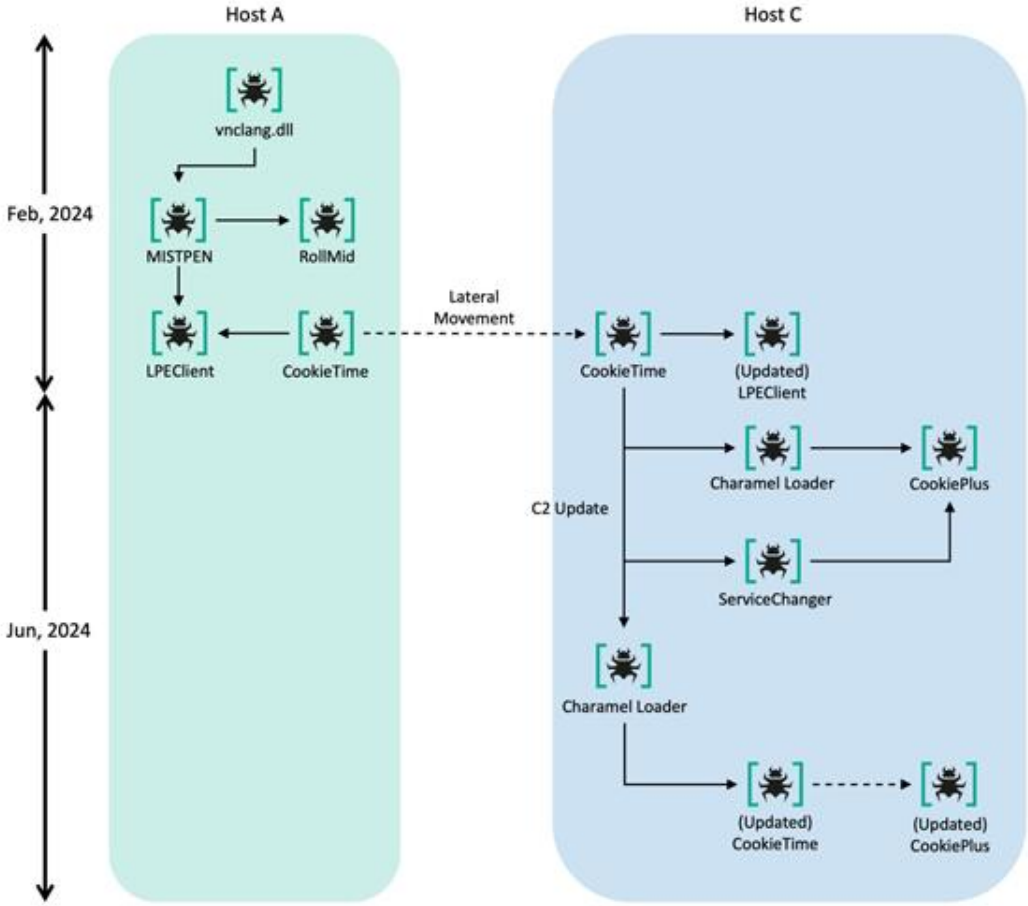
Cabe destacar que el uso por parte del Grupo Lazarus de versiones maliciosas de aplicaciones VNC para atacar a ingenieros nucleares ya había sido resaltado por Kaspersky en octubre de 2023 en su informe de tendencias de amenazas avanzadas persistentes (APT) para el tercer trimestre de 2023.

> *«Lazarus entregó el primer archivo comprimido a al menos dos personas dentro de la misma organización (a las que llamaremos Host A y Host B). Después de un mes, intentaron ataques más intensivos contra el primer objetivo»*, dijeron los investigadores Vasily Berdnikov y Sojun Ryu.

Las aplicaciones VNC, una versión troyanizada de TightVNC llamada AmazonVNC.exe, se distribuyeron en forma de imágenes ISO y archivos ZIP. En otros casos, se utilizó una versión legítima de UltraVNC para cargar una DLL maliciosa empaquetada dentro del archivo ZIP.

La DLL (vnclang.dll) actúa como un cargador para un backdoor denominado MISTPEN, descubierto por Mandiant, propiedad de Google, en septiembre de 2024. Esta actividad está siendo rastreada bajo el nombre UNC2970. Por su parte, MISTPEN ha sido asociado con la entrega de dos cargas adicionales apodadas RollMid y una nueva variante de LPEClient.

Kaspersky también observó que el malware CookieTime fue implementado en el Host A, aunque se desconoce el método exacto utilizado para lograrlo. Descubierto por primera vez en septiembre y noviembre de 2020, CookieTime debe su nombre al uso de valores de cookies codificados en solicitudes HTTP para recibir instrucciones de un servidor de comando y control (C2).



Se ha revelado que la investigación más profunda de la cadena de ataque mostró que el actor de amenazas se movió lateralmente desde el Host A a otra máquina (Host C), donde nuevamente se utilizó CookieTime para desplegar diversos *payloads* entre febrero y junio de 2024, como se detalla a continuación:

- LPEClient: un malware diseñado para recopilar información sobre los hosts comprometidos.
- ServiceChanger: un malware que detiene un servicio legítimo específico para cargar una DLL maliciosa mediante la técnica de *DLL side-loading*.
- Charamel Loader: un *loader* de malware que descifra y carga recursos internos como CookieTime, CookiePlus y ForestTiger.

- CookiePlus: un programa malicioso basado en plugins que es cargado tanto por ServiceChanger como por Charamel Loader.

> *«La diferencia entre cada CookiePlus cargado por Charamel Loader y ServiceChanger radica en la forma en que se ejecuta. El primero opera como una DLL independiente e incluye la información de C2 en su sección de recursos»*, señalaron los investigadores.
>
> *«El segundo extrae información almacenada en un archivo externo, como msado.inc, lo que significa que CookiePlus tiene la capacidad de obtener una lista de C2 tanto de un recurso interno como de un archivo externo. Por lo demás, el comportamiento es el mismo.»*

CookiePlus recibe su nombre porque inicialmente se disfrazó como un plugin de código abierto para Notepad++ llamado ComparePlus cuando fue detectado en el entorno real por primera vez. En los ataques dirigidos contra una entidad relacionada con el ámbito nuclear, se descubrió que estaba basado en otro proyecto llamado DirectX-Wrappers.

El malware actúa como un descargador para recuperar un *payload* codificado en Base64 y cifrado con RSA desde el servidor C2, el cual luego se decodifica y descifra para ejecutar tres *shellcodes* diferentes o una DLL. Los *shellcodes* están diseñados para recopilar información del sistema y hacer que el módulo principal de CookiePlus entre en un estado de reposo durante un tiempo determinado.

Se sospecha que CookiePlus es el sucesor de MISTPEN debido a las similitudes en su comportamiento, incluyendo el hecho de que ambos se han disfrazado como plugins de Notepad++.

> *«A lo largo de su historia, el grupo Lazarus ha utilizado solo un pequeño número de marcos de malware modulares como Mata y Gopuram Loader», señaló Kaspersky.*

> *«El hecho de que estén introduciendo nuevos malwares modulares, como CookiePlus, sugiere que el grupo trabaja constantemente en mejorar su arsenal y sus cadenas de infección para evadir la detección de los productos de seguridad.»*

Estos hallazgos coinciden con el informe de la firma de inteligencia blockchain Chainalysis, que reveló que actores de amenazas afiliados a Corea del Norte han robado $1.34 mil millones en 47 ataques a criptomonedas en 2024, frente a los $660.5 millones de 2023. Esto incluye el ataque de mayo de 2024 a la bolsa japonesa de criptomonedas DMM Bitcoin, que sufrió una pérdida de $305 millones en ese momento.

> *«Lamentablemente, parece que los ataques de criptomonedas de la RPDC están volviéndose más frecuentes. En particular, los ataques de entre $50 y $100 millones, así como los superiores a $100 millones, ocurrieron con mucha más frecuencia en 2024 que en 2023, lo que sugiere que la RPDC está mejorando y acelerando sus grandes explotaciones»*, señaló la compañía.