El grupo Lazarus, asociado a Corea del Norte y también conocido como Hidden Cobra o TEMP.Hermit, ha sido detectado utilizando versiones manipuladas de aplicaciones de Virtual Network Computing (VNC) como cebos para atacar a la industria de defensa e ingenieros nucleares en el marco de una campaña de larga duración denominada Operación Dream Job.

> *«El actor de amenazas engaña a personas que buscan empleo en redes sociales para que abran aplicaciones maliciosas en entrevistas de trabajo ficticias»,* según señala Kaspersky en su informe de tendencias de APT para el tercer trimestre de 2023.

> *«Para eludir la detección por parte de soluciones de seguridad basadas en el comportamiento, esta aplicación con puerta trasera opera de manera discreta, activándose únicamente cuando el usuario selecciona un servidor en el menú desplegable del cliente VNC manipulado».*

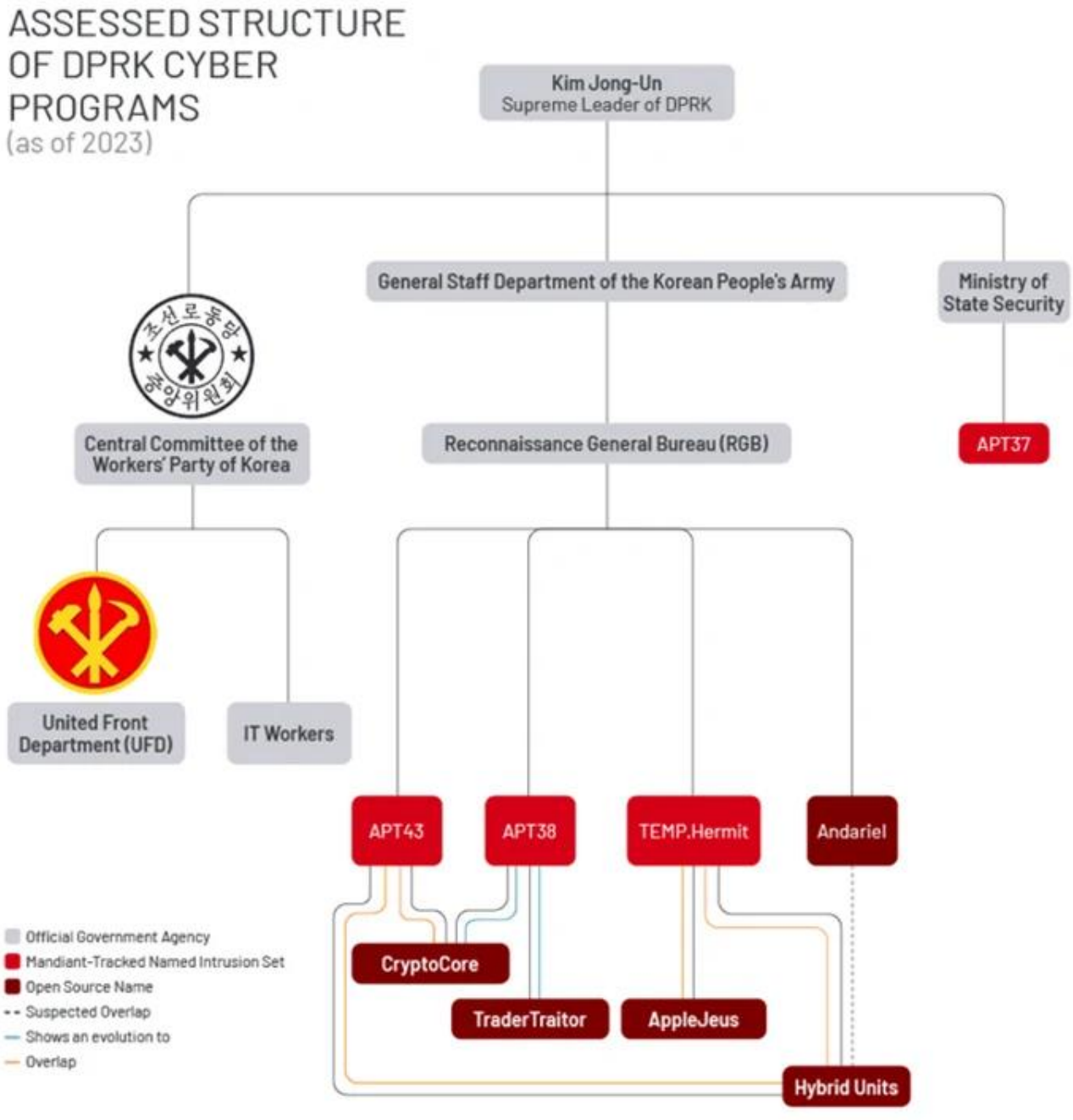
Una vez activada por la víctima, la aplicación falsa está diseñada para recuperar componentes adicionales, incluyendo un malware reconocido del grupo Lazarus denominado LPEClient, que posee capacidades para perfilar hosts comprometidos.

El atacante también implementa una versión actualizada de COPPERHEDGE, una puerta trasera conocida por ejecutar comandos arbitrarios, llevar a cabo reconocimiento del sistema y extraer datos, además de un malware personalizado destinado específicamente a transmitir archivos de interés a un servidor remoto.

Los objetivos de la última campaña incluyen empresas directamente relacionadas con la fabricación de productos de defensa, como sistemas de radar, vehículos aéreos no tripulados (UAVs), vehículos militares, barcos, armamento y compañías marítimas.

Operación Dream Job hace referencia a una serie de ataques orquestados por el grupo de

piratería norcoreano, en los cuales los posibles objetivos son contactados a través de cuentas sospechosas en varias plataformas, como LinkedIn, Telegram y WhatsApp, bajo el pretexto de ofrecer oportunidades laborales atractivas con el fin de engañarlos para que instalen malware.




A finales del mes pasado, ESET reveló detalles de un ataque del grupo Lazarus dirigido a una empresa aeroespacial no nombrada en España, en el que empleados de la firma fueron

abordados por el actor de amenazas que se hacía pasar por un reclutador de Meta en LinkedIn para entregar un implante llamado LightlessCan.

El grupo Lazarus es solo uno de los varios programas ofensivos originarios de Corea del Norte que se han relacionado con actividades de espionaje cibernético y robos con motivación financiera.

Otro destacado grupo de piratería es APT37, también conocido como ScarCruft, que forma parte del Ministerio de Seguridad del Estado, a diferencia de otros grupos de actividad amenazante, como APT43, Kimsuky y el grupo Lazarus (y sus subgrupos Andariel y BlueNoroff), que están afiliados a la Oficina General de Reconocimiento (RGB).

> *«A pesar de que distintos grupos de amenazas comparten herramientas y código, la actividad amenazante norcoreana sigue adaptándose y cambiando para crear malware personalizado para diferentes plataformas, incluyendo Linux y macOS»,* reveló Mandiant, propiedad de Google, a principios de este mes, resaltando su evolución en términos de adaptabilidad y complejidad.

ScarCruft, según Kaspersky, atacó a una empresa comercial vinculada a Rusia y Corea del Norte utilizando una novedosa cadena de ataque de phishing que culminó con la entrega del malware RokRAT, también conocido como BlueLight, enfatizando los continuos intentos del reino ermitaño de dirigirse a Rusia.

Además, otro cambio notable es la superposición de infraestructura, herramientas y objetivos entre varios grupos de piratería norcoreanos, como Andariel, APT38, el grupo Lazarus y APT43, lo que complica los esfuerzos de atribución y apunta a una racionalización de las actividades adversarias.

Esto también ha venido acompañado de un *«incremento en el interés por desarrollar malware para macOS para acceder a plataformas de alto valor en las industrias de criptomonedas y blockchain»,* según Mandiant.