Una campaña de espionaje cibernético dirigida a los sectores aeroespacial y de defensa para instalar implantes de recopilación de datos en las máquinas de las víctimas con fines de vigilancia y exfiltración de datos, puede haber sido más sofisticada de lo que antes se creía.

Los ataques, que tenían como objetivo direcciones IP pertenecientes a proveedores de servicios de Internet (ISP) en Australia, Israel, Rusia y contratistas de defensa con sede en Rusia e India, involucraron una herramienta de software espía no descubierta anteriormente llamada Torisma, para monitorear sigilosamente a sus víctimas en busca de explotación continua.

Rastreada bajo el nombre en clave de «*North Star Operation*«, por investigadores de McAfee, los hallazgos iniciales de la campaña en julio revelaron el uso de sitios de redes sociales, spear-phishing y documentos armados con ofertas de trabajo falsas para engañar a los empleados que trabajan en el sector de defensa para obtener ganancias.

Los ataques se han atribuido a la infraestructura y los TTP (Técnicas, Tácticas y Procedimientos) previamente asociados con Hidden Cobra, un término utilizado por el gobierno de Estados Unidos para describir a todos los grupos de piratas informáticos patrocinados por el estado de Corea del Norte.

El desarrollo sigue la tendencia de Corea del Norte, un país fuertemente sancionado, que aprovecha su arsenal de actores de amenazas para apoyar y financiar su programa de armas nucleares perpetrando ataques maliciosos contra los contratistas aeroespaciales y de defensa de Estados Unidos.

Aunque el análisis inicial sugirió que los implantes estaban destinados a recopilar información básica de las víctimas para evaluar su valor, la última investigación sobre la Operación North Star, exhibe un *«grado de innovación técnica»* diseñado para permanecer oculto en los sistemas comprometidos.

La campaña no solo utilizó contenido legítimo de contratación de empleo de los sitios web populares de contratistas de defensa de Estados Unidos para atraer a las víctimas seleccionadas a abrir archivos adjuntos de correo electrónico de spear-phihing, sino que los atacantes comprometieron y utilizaron sitios web genuinos en Estados Unidos e Italia, como una casa de subastas, una imprenta y una empresa de capacitación en TI, para albergar sus capacidades de comando y control (C2).

> *«El uso de estos dominios para realizar operaciones C2 probablemente les permitió eludir las medidas de seguridad de algunas organizaciones porque la mayoría de las organizaciones no bloquean los sitios web confiables»*, dijeron los investigadores de McAfee, Christian Beek y Ryan Sherstibitoff.

Además, el implante de primera etapa incrustado en los documentos de Word seguiría evaluando los datos del sistema de la víctima, como la fecha, dirección IP, agente de usuario, etcétera, mediante la verificación cruzada con una lista predeterminada de direcciones IP de destino para instalar un segundo implante llamado Torisma, minimizando al mismo tiempo el riesgo de detección y descubrimiento.

Este implante de monitoreo especializado se utiliza para ejecutar shellcode personalizado, además de monitorear activamente las nuevas unidades agregadas al sistema, así como las conexiones de escritorio remoto.

> *«Esta campaña fue interesante porque había una lista particular de objetivos de interés, y esa lista se verificó antes de que se tomara la decisión de enviar un segundo implante, ya sea de 32 o 64 bits, para un monitoreo adicional y en profundidad»*, dijeron los investigadores.

> *«El progreso de los implantes enviados por el C2 fue monitoreado y escrito en un archivo de registro que le dio al adversario una descripción general de las víctimas*

> *que se infiltraron con éxito y se pudieron monitorear más»,* agregaron.