El Equipo de Intervención en Situaciones de Ciberemergencias de Ucrania (CERT-UA) ha lanzado una alerta sobre una reciente estrategia de phishing dirigida por el grupo APT28, que tiene conexiones con Rusia. Este grupo busca difundir software malicioso no identificado previamente, como OCEANMAP, MASEPIE y STEELHOOK, con el propósito de obtener datos confidenciales.

La entidad gubernamental identificó esta actividad entre el 15 y el 25 de diciembre de 2023, enfocándose principalmente en instituciones gubernamentales mediante correos electrónicos que animan a los usuarios a abrir un enlace para revisar un documento.

Pero, en una jugada astuta, esos enlaces llevan a sitios web maliciosos que explotan características de JavaScript y el protocolo URI «search-ms:». Estos sitios descargan un archivo atajo de Windows (LNK), que a su vez ejecuta instrucciones de PowerShell para iniciar una serie de infecciones con el malware recién descubierto, MASEPIE.

MASEPIE es una utilidad programada en Python que facilita la descarga y subida de archivos, y la ejecución de comandos. Establece comunicaciones con un servidor de control y comando (C2) de forma segura mediante el protocolo TCP.

Estas tácticas también abren el camino para otros programas maliciosos, como un script de PowerShell denominado STEELHOOK, que tiene la capacidad de extraer información del historial del navegador y enviarla a un servidor bajo control de un tercero, cifrando los datos en formato Base64.

Además, se introduce una herramienta maliciosa escrita en C# llamada OCEANMAP, que se encarga de ejecutar órdenes mediante cmd.exe.

CERT-UA indicó: *«Se emplea el protocolo IMAP como vía de comunicación»,* añadiendo que la persistencia se establece al crear un archivo de URL titulado «VMSearch.url» en el directorio de inicio de Windows.

> *«Los comandos codificados en Base64 se encuentran en los 'Borradores' de los correos; cada borrador identifica la máquina, el usuario y la versión del sistema operativo. Las respuestas a estos comandos se archivan en el directorio principal.»*

La entidad resaltó que, tras el acceso inicial, se inician rápidamente tareas de reconocimiento y movimientos laterales usando herramientas como Impacket y SMBExec.

Estas revelaciones emergen poco después de que IBM X-Force informara sobre el uso por parte de APT28 de señuelos relacionados con el conflicto Israel-Hamas para promover un troyano personalizado llamado HeadLace.

Recientemente, se ha vinculado al activo grupo de hackers apoyado por el gobierno ruso con la explotación de un defecto de seguridad crítico, ya corregido, en el servicio de correo electrónico Outlook (CVE-2023-23397, calificado con una puntuación CVSS de 9.8) para infiltrarse en cuentas de servidores Exchange.