Investigadores de seguridad cibernética revelaron el jueves los detalles de una puerta trasera de Windows en memoria no descubierta, previamente desarrollada por una operación de hackers a sueldo que puede ejecutar código malicioso remotamente y robar información confidencial de sus objetivos en Asia, Europa y Estados Unidos.

Apodado como PowerPepper por investigadores de Kaspersky, el malware se ha atribuido al grupo DeathStalker, antes llamado Deceptikons, un actor de amenazas que se ha encontrado afectando a bufetes de abogados y empresas del sector financiero ubicados en Europa y Oriente Medio desde al menos 2012.

La herramienta de piratería se llama así debido a su dependencia de los trucos esteganográficos para entregar la carga útil de la puerta trasera en forma de una imagen de helechos o pimientos.

El grupo de espionaje se hizo público por primera vez a inicios de julio, y la mayoría de sus ataques comenzaron con un correo electrónico de phishing que contenía un archivo LNK modificado malicioso que, al hacer clic, descarga y ejecuta un implante basado en PowerShell, llamado Powersing.

Aunque sus objetivos no parecen estar motivados económicamente, su continuo interés en recopilar información confidencial crucial llevó a Kaspersky a la conclusión de que *«DeathStalker es un grupo de mercenarios que ofrecen servicios de piratería informática a sueldo o que actúan como una especie de intermediario de información en círculos financieros»*.

PowerPepper ahora se une a la lista del grupo de conjuntos de herramientas en expansión y evolución.

Descubierta en estado activo a mediados de julio de 2020, esta nueva cepa de malware se elimina de un documento de Word señuelo y aprovecha DNS sobre HTTPS (DoH) como un canal de comunicación para transmitir comandos de shell maliciosos cifrados desde un servidor controlado por un atacante.

Los correos electrónicos de spear-phishing se pueden encontrar en temas tan variados como regulaciones de emisión de carbono, reserva de viajes y la pandemia de coronavirus en curso, y los documentos de Word tienen pancartas de ingeniería social que instan a los usuarios a habilitar macros en un intento por atraer a un usuario desprevenido para que descargue la puerta trasera.

Para lograr sus objetivos, el implante envía solicitudes de DNS a servidores de nombres (servidores que almacenan registros de DNS) asociados con un dominio C2 malicioso, que luego devuelve el comando para que se ejecute en forma de respuesta incorporada. Luego de la ejecución, los resultados se transmiten al servidor a través de un lote de solicitudes de DNS.

Además de aprovechar las cadenas de distribución basadas en macros y LNK para implementar el malware, DeathStalker empleó *«trucos de ofuscación, ejecución y enmascaramiento para dificultar la detección o engañar a los objetivos que sienten curiosidad por lo que está sucediendo en sus computadoras»*, dijo Pierre Delcher de Kaspersky.

Entre las principales características del malware, destaca su forma de ocultar el flujo de trabajo de ejecución maliciosa en las propiedades de objetos y formas incrustadas de Word y utilizar archivos de ayuda HTML compilada (CHM) de Windows como archivos maliciosos.

Se han visto múltiples grupos mercenarios en la naturaleza antes, incluidos BellTroX (también conocido como Dark Basin), Bahamut y CostaRicto, todos los cuales, han implementado malware personalizado para violar sistemas que pertenecen a instituciones financieras y funcionarios gubernamentales.

> *«Parece justo escribir que DeathStalker se esforzó por desarrollar herramientas evasivas, creativas e intrincadas con este implante PowerPepper y las cadenas de suministro asociadas»,* dijo Delcher.

> *«No hay nada particularmente sofisticado en las técnicas y trucos que se aprovechan, sin embargo, todo el conjunto de herramientas ha demostrado ser efectivo, está bastante bien elaborado y muestra esfuerzos decididos para comprometer varios objetivos en todo el mundo»*, agregó.

Para protegerse contra la entrega y ejecución de PowerPepper, se recomienda que las empresas y los usuarios actualicen sus backends de CMS, así como los complementos asociados, restrinjan el uso de PowerShell en computadoras de usuarios finales con políticas de ejecución impuesta y se abstengan de abrir accesos directos de Windows adjuntos a correos electrónicos o hacer clic en enlaces de correos electrónicos de remitentes desconocidos.