Se ha atribuido a una parte de un grupo de estado-nación iraní conocido como Nemesis Kitten, estar detrás de un malware personalizado previamente no documentado denominado Drokbk, que usa GitHub como un resolutor de punto muerto para filtrar datos de una computadora infectada o para recibir comandos.

> *«El uso de GitHub como punto muerto virtual ayuda a que el malware se mezcle. Todo el tráfico a GitHub está encriptado, lo que significa que las tecnología defensivas no pueden ver lo que se pasa de un lado a otro. Y debido a que GitHub es un servicio legítimo, plantea menos preguntas»,* dijo Rafe Pilling, investigador principal de Secureworks.

Las actividades maliciosas del actor patrocinado por el gobierno iraní pasaron desapercibidas a inicios de febrero de 2022, cuando se observó que explotaba las vulnerabilidades de Log4Shell en servidores VMware Horizon sin parches para implementar ransomware.

Nemesis Kitten es rastreado por la comunidad de seguridad cibernética más grande bajo varios nombres como TunnelVision, Cobalt Mirage y UNC2448. También es un subclúster del grupo Phosphorus, demás de la designación DEV-0270 por parte de Microsoft.

Además, se dice que comparte superposiciones tácticas con otro colectivo adversario denominado Cobalt Illusion (también conocido como APT42), un subgrupo de Phosphorus que *«tiene la tarea de realizar operaciones de vigilancia y recopilación de información contra personas y organizaciones de interés estratégico para el gobierno iraní».*

Investigaciones posteriores sobre las operaciones del adversario descubrieron dos conjuntos de intrusión distintos: el Grupo A, que emplea BitLocker y DiskCryptor para realizar ataques de ransomware oportunistas para obtener ganancias financieras, y el Grupo B, que lleva a cabo robos dirigidos para recopilar inteligencia.

Desde entonces, Microsoft, Google, Mandiant y Secureworks descubrieron pruebas que rastrean los orígenes de Cobalt Mirage hasta dos empresas fachada iraníes, Najee

Technology y Afkar System, que, según el Departamento del Tesoro de Estados unidos, están afiliadas al Cuerpo de la Guardia Revolucionaria Islámica (IRGC).

Drokbk, el malware recientemente identificado, está asociado con el Clúster B y está escrito en .NET. Se implementó después de la explotación como una forma de establecer la persistencia, consta de un cuentagotas y una carga útil que se usa para ejecutar los comandos recibidos de un servidor remoto.

> *«Los primeros signos de su uso en la naturaleza aparecieron en una intrusión en febrero de 2022 en una red del gobierno local de Estados Unidos»,* dijo la compañía de seguridad cibernética.

Este ataque implicó el compromiso de un servidor VMware Horizon utilizando las vulnerabilidades Log4j (CVE-2021-44228 y CVE-2021-45046), lo que finalmente condujo a la entrega del binario Drokbk por medio de un archivo ZIP comprimido alojado en un servicio de transferencia de archivos.

Como medida de evasión de detección, Drokbk emplea una técnica llamada resolución de caída muerta para determinar su servidor de comando y control (C2). La táctica encubierta se refiere al uso de un servicio web externo legítimo existente para alojar información que apunta a una infraestructura C2 adicional.

En la cadena de ataques observada por Secureworks, esto se logra aprovechando un repositorio de GitHub controlado por atacantes que contiene la información del servidor C2 dentro del archivo README.md.

> *«Drokbk proporciona a los actores de amenazas acceso remoto arbitrario y un punto de apoyo adicional junto con herramientas de tunelización como Fast Reverse (FRP) y Ngrok»,* dijo Pilling.