En una impactante revelación, resulta que un grupo de personas ha utilizado las vulnerabilidades de día cero relacionadas con el Equation Group de la NSA, casi un año antes de que el misterioso grupo de Agentes de la Sombra los filtrara.

Según un nuevo informe publicado por la compañía de seguridad cibernética Symantec, un grupo vinculado a los chinos, llamado Buckeye, estaba utilizando las herramientas de piratería vinculadas a la NSA desde marzo de 2016, mientras que los Shadow Brokers abandonaron algunas de las herramientas en Internet en abril de 2017.

Activo desde 2009, Buckeye, también conocido como APT3, Gothic Panda, UPS Team y TG-0110, es responsable de una gran cantidad de ataques de espionaje, principalmente contra organizaciones críticas y de defensa en los Estados Unidos.

Aunque Symantec no mencionó de forma explícita a China en su informe, los investigadores con alto grado de confianza han atribuido previamente [1,2] al grupo de piratería Buckeye a una empresa de seguridad de información, llamada *Boyusec*, que trabaja en nombre del Ministerio de Seguridad de China.

El último descubrimiento de Symantec proporciona la primera evidencia de que los piratas informáticos chinos patrocinados por el estado lograron adquirir algunas de las herramientas de piratería, incluidas EternalRomance, EternalSynergy y DoublePulsar, un año antes de ser abandonados por los Shadow Brokers, un grupo misterioso que aún no se ha identificado.

Según los investigadores, el grupo Buckeye usó su herramienta de explotación personalizada, llamada Bemstour, para entregar una variante del implante de puerta trasera DoublePulsar para recopilar sigilosamente información y ejecutar código malicioso en las computadoras seleccionadas.

La herramienta Benstour fue diseñada para explotar dos vulnerabilidades de día cero (CVE-2019-0703 y CVE-2017-0143) en Windows para lograr la ejecución remota de código de kernel en las computadoras específicas.

Microsoft abordó la vulnerabilidad CVE-2017-0143 en marzo de 2017 después de que se descubrió que fue utilizada por dos explotaciones de la NSA que fueron filtradas por Shadow Brokers.

La falla desconocida del servidor SMB de Windows (CVE-2019-0703) fue descubierta e informada por Symantec a Microsoft en septiembre de 2018 y fue reparada por la compañía el mes pasado.

Los investigadores detectaron a los hackers de BuckEye utilizando la combinación del exploit SMB y la puerta trasera DoublePulsar para dirigirse a las compañías de telecomunicaciones, así como a las instituciones de investigación científica y educación en Hong Kong, Luxemburgo, Bélgica, Filipinas y Vietnam, desde marzo de 2016 hasta agosto de 2017.

¿Cómo obtuvieron los chinos las herramientas de hacking de la NSA?

Aunque Symantec no sabe cómo los hackers chinos obtuvieron las herramientas de Equation Group antes de la filtración de Shadow Brokers, la firma de seguridad afirma que existe la posibilidad de que BuckEye haya capturado el código de un ataque de la NSA en sus propias computadoras y luego diseñó el malware de ingeniería inversa para desarrollar su propia versión de dichas herramientas.

> *«Otros escenarios menos compatibles, dada la evidencia técnica disponible, incluyen que BuckEye obtenga las herramientas al obtener acceso a un servidor de Equation Group no asegurado o con poca seguridad, o que un miembro de Equation Group no autorizado haya filtrado las herramientas a BuckEye»*, dijo Symantec.

BuckEye suspendió sus operaciones a mediados de 2017, o al menos eso pareció, y tres supuestos miembros del grupo fueron acusados en noviembre de 2017. Sin embargo, las herramientas de Bemstour y DoublePulsar utilizadas por BuckEye siguieron siendo utilizadas hasta finales de 2018 en conjunto con distintos programas maliciosos.

Aunque se desconoce quién siguió utilizando las herramientas, los investigadores creen que el grupo BuckEye pudo haber pasado algunas de sus herramientas a otro grupo, o *«siguió operando más de lo que se suponía».*

Luego de la filtración de Shadow Brokers, los hackers norcoreanos y la inteligencia rusa utilizaron las herramientas de explotación vinculadas a la NSA, aunque el informe de Symantec no sugiere una conexión aparente entre la adquisición de herramientas por parte de BuckEye y la filtración de Shadow Brokers.