Una botnet activa que comprende cientos de miles de sistemas secuestrados distribuidos en 30 países, está explotando «*docenas de vulnerabilidades conocidas*» para atacar sistemas de administración de contenido (CMS) ampliamente utilizados.

La campaña, llamada KashmirBlack, que se cree que comenzó al rededor de noviembre de 2019, apunta a plataformas de CMS populares como WordPress, Joomla, PrestaShop, Magento, Drupal, Vbulletin, OsCommerence, OpenCart y Yeager.

> *«Su infraestructura bien diseñada hace que sea fácil expandir y agregar nuevos exploits o cargas útiles sin mucho esfuerzo, y utiliza métodos sofisticados para camuflarse, no ser detectado y proteger su operación»,* dijeron los investigadores de Imperva en su análisis.

La investigación de seis meses de la compañía de seguridad sobre la botnet, revela una operación compleja administrada por un servidor de comando y control (C2) y más de 60 servidores sustitutos que se comunican con los bots para enviar nuevos objetivos, lo que permite expandir el tamaño de la botnet mediante ataques de fuerza bruta e instalación de puertas traseras.

El propósito principal de KashmirBlack es abusar de los recursos de los sistemas comprometidos para la minería de criptomonedas Monero y redirigir el tráfico legítimo de un sitio web a páginas de spam. Pero también se aprovecha para llevar a cabo ataques de defacing.

Independientemente del motivo, los intentos de explotación comienzan con el uso de la vulnerabilidad PHPUnit RCE (CVE-2017-9841) para infectar a los clientes con cargas útiles maliciosas de próxima etapa que se comunican con el servidor C2.

Basado en la firma del ataque que se encontró durante algunas desfiguraciones, los investigadores de Imperva dijeron que creían que la botnet era obra de un hacker llamado Exect1337, un miembro de la tripulación de hackers de Indonesia, PhantomGhost.

La infraestructura de KashmirBlack es compleja y comprende una serie de partes móviles, incluidos dos repositorios separados: uno para alojar exploits y cargas útiles, y el otro para almacenar el script malicioso para la comunicación con el servidor C2.

Los propios robots están designados como un *«bot de propagación»,* un servidor víctima que se comunica con el C2 para recibir comandos para infectar a nuevas víctimas, o un *«bot pendiente»,* una víctima recientemente comprometida cuyo propósito en la botnet aún no está definido.

Aunque CVE-2017-9841 se utiliza para convertir a una víctima en un bot que se propaga, la explotación exitosa de 15 fallas diferentes en los sistemas CMS lleva a que el sitio de la víctima se convierta en un nuevo bot pendiente en la botnet. Los operadores de KashmirBlack han empleado una vulnerabilidad de carga de archivos WebDAV separada para provocar la desfiguración.

Pero justo cuando la botnet creció en tamaño y más bots comenzaron a obtener cargas útiles de los repositorios, la infraestructura se modificó para hacerla más escalable al agregar una entidad de equilibrador de carga que devuelve la dirección de uno de los repositorios redundantes recién configurados.

El mes pasado, los investigadores encontraron que la botnet usaba Dropbox como reemplazo de su infraestructura C2, abusando de la API del servicio de almacenamiento en la nube para obtener instrucciones de ataque y cargar informes de ataque de los bots que se propagan.

> *«Pasar a Dropbox permite a la botnet ocultar la actividad delictiva ilegítima detrás de servicios web legítimo. Es un paso más hacia el camuflaje del tráfico de la botnet, asegurando la operación de C&C, y lo más importante, dificultando el rastreo de la botnet hasta el pirata informático que está detrás de la operación»,* dijo Imperva.