Un grupo de hackers de acceso inicial rastreado como Prophet Spider, fue vinculado a un conjunto de actividades maliciosas que explotan la vulnerabilidad Log4Shell en servidores VMware Horizon sin parches.

Según una nueva investigación publicada hoy por los equipos de BlackBerry Research & Intelligence e Incident Response (IR), los atacantes han estado aprovechando de forma oportunista la vulnerabilidad para descargar una carga útil de segunda etapa en los sistemas víctimas.

Las cargas útiles observadas incluyen mineros de criptomonedas, Cobalt Strike Beacons y web shells, lo que corrobora un aviso anterior del Servicio Nacional de Salud (NHS) del Reino Unido, que hizo sonar la alarma sobre la explotación activa de las vulnerabilidades en los servidores VMware Horizon para lanzar web shells maliciosos y establecer persistencia en las redes afectadas para los ataques de seguimiento.

Log4Shell es un apodo que se usa para referirse a un exploit que afecta a la popular biblioteca Apache Log4j y que da como resultado la ejecución remota de código mediante el registro de una cadena especialmente diseñada.

Desde la divulgación pública de la falla el mes pasado, los actores de amenazas se apresuraron a implementar este nuevo vector de ataque para una variedad de campañas de intrusión para obtener el control total de los servidores afectados.

BlackBerry dijo que observó instancias de explotación de tácticas, técnicas y procedimientos (TTP) que se atribuían previamente al cártel Prophet Spider eCrime, incluido el uso de la ruta de la carpeta «C:\Windows\Temp\7fde\» para almacenar archivos maliciosos y «wget .bin», ejecutable para obtener binarios adicionales, así como superposiciones en la infraestructura utilizada por el grupo.

«Prophet Spider obtiene acceso a las víctimas principalmente al comprometer servidores web vulnerables y utiliza una variedad de herramientas de baja prevalencia para lograr objetivos operativos», dijo CrowdStrike en agosto de 2021, cuando se vio al grupo explotando

activamente fallas en los servidores Oracle WebLogic para obtener acceso inicial a los entornos de destino.

Al igual que con muchos otros corredores de acceso inicial, los puntos de apoyo se venden al mejor postor en foros clandestinos ubicados en la dark net, que luego explotan el acceso para la implementación de ransomware. Se sabe que Prophet Spider está activo desde al menos mayo de 2017.

Esto está lejos de ser la primera vez que los sistemas orientados a Internet que ejecutan VMWare Horizon han sido atacados utilizando exploits Log4Shell. A inicios del mes, Microsoft llamó a un operador con sede en China rastreado como DEV-0401 por implementar una nueva cepa de ransomware llamada NightSky en los servidores comprometidos.

La embestida contra los servidores de Horizon también llevó a VMware a instar a sus clientes a aplicar los parches de inmediato. *«Las ramificaciones de esta vulnerabilidad son serias para cualquier sistema, especialmente los que aceptan tráfico de la Internet abierta»,* dijo el proveedor de servicios de virtualización.

> *«Cuando un grupo de corredores de acceso se interesa en una vulnerabilidad cuyo alcance es tan desconocido, es una buena indicación de que los atacantes ven un valor significativo en su explotación»*, dijo Tony Lee, vicepresidente de operaciones técnicas de servicios globales de BlackBerry.

> *«Es probable que sigamos viendo grupos criminales explorando las oportunidades de la vulnerabilidad Log4Shell, por lo que es un vector de ataque contra el cual los defensores deben ejercer una vigilancia constante»,* agregó Lee.