La división de inteligencia de amenazas de Microsoft evaluó el miércoles que un subgrupo del atacante iraní rastreado como Phosphorus, está realizando ataques de ransomware como una *«forma de pluriempleo»* para beneficio personal.

Microsoft, que está monitoreando el grupo de actividades bajo el nombre de DEV-0270 (también conocido como Nemesis Kitten), dijo que es operado por una compañía que funciona bajo los alias públicos Secnerd y Lifeweb, citando superposiciones de infraestructura entre el grupo y las dos organizaciones.

> *«DEV-0270 aprovecha las vulnerabilidades de alta gravedad para obtener acceso a los dispositivos y es conocido por la adopción temprana de vulnerabilidades recientemente reveladas»,* dijo Microsoft.

> *«DEV-0270 también usa ampliamente los archivos binarios que viven fuera de la tierra (LOLBIN) a lo largo de la cadena de ataque para el descubrimiento y el acceso de credenciales. Esto se extiende a su abuso de la herramienta integrada BitLocker para cifrar archivos en dispositivos comprometidos».*

El uso de BitLocker y DiskCryptor por parte de atacantes iraníes para ataques de ransomware oportunistas salió a la luz a inicios de mayo, cuando Secureworks reveló un conjunto de intrusiones montadas por un grupo de amenazas que rastrea bajo el nombre de Cobalt Mirage con vínculos con Phosphorus (también conocido como Cobalt Illusion) y TunnelVision.

Se sabe que DEV-0270 escanea Internet para encontrar servidores y dispositivos susceptibles a fallas en Microsoft Exchange Server, Fortinet FortiGate SSL-VPN y Apache Log4j para obtener acceso inicial, seguido de actividades de reconocimiento de red y robo de credenciales.

El acceso a la red comprometida se logra estableciendo persistencia por medio de una tarea

programada. Después, DEV-0270 eleva los privilegios al nivel del sistema, lo que le permite realizar acciones posteriores a la explotación, como deshabilitar Microsoft Defender Antivirus para evadir la detección, el movimiento lateral y el cifrado de archivos.

> *«El grupo de amenazas comúnmente usa comandos nativos WMI, net, CMD y PowerShell, y configuraciones de registro para mantener el sigilo y la seguridad operativa. También instalan y enmascaran sus archivos binarios personalizados como procesos legítimos para ocultar su presencia»,* dijo Microsoft.

Se recomienda a los usuarios que prioricen la aplicación de parches a los servidores de Exchange con acceso a Internet para mitigar el riesgo, restringir los dispositivos de red como los dispositivos SSL-VPN de Fortinet para que no realicen conexiones arbitrarias a Internet, aplicar contraseñas seguras y mantener copias de seguridad periódicas de los datos.