Un ataque cibernético reciente del malware IceID permitió al actor de amenazas comprometer el dominio de Active Directory de un objetivo sin nombre menos de 24 horas después de obtener el acceso inicial.

> *«A lo largo del ataque, el atacante siguió una rutina de comandos de reconocimiento, robo de credenciales, movimiento lateral, abusando de los protocolos de Windows y ejecutando Cobalt Strike en el host recién comprometido»,* dijeron los investigadores de Cybereason en un informe.

IceID, también conocido con el nombre de BokBot, comenzó su vida como un troyano bancario en 2017 antes de convertirse en un gotero para otro malware, uniéndose a Emotet, TrickBot, Qakbot, Bumblebe y Raspberry Robin.

Los ataques que involucran la entrega de IceID aprovecharon una variedad de métodos, especialmente a raíz de la decisión de Microsoft de bloquear las macros de los archivos de Office descargados de la web.

La intrusión detallada por Cybereason no es distinta en el sentido de que la cadena de infección comienza con un archivo de imagen ISO contenido dentro de un archivo ZIP que culmina con la ejecución de la carga útil de IceID.

Después, el malware establece persistencia en el host por medio de una tarea programada y se comunica con un servidor remoto para descargar cargas útiles adicionales, incluyendo Cobalt Strike Beacon para la actividad de reconocimiento de seguimiento.

También realiza un movimiento lateral a través de la red y ejecuta el mismo Cobalt Strike Beacon en todas esas estaciones de trabajo, y después procede a instalar el Agente Atera, una herramienta legítima de administración remota, como un mecanismo de acceso remoto redundante.

> *«Utilizar herramientas de TI como esta permite a los atacantes crear una 'puerta trasera' adicional para ellos mismos en caso de que se descubran y reparen sus mecanismos de persistencia iniciales. Es menos probable que estas herramientas sean detectadas por antivirus o EDR y también es más probable que se descarten como falsos positivos»,* dijeron los investigadores.

Cobalt Strike Beacon se usa además como un conducto para descargar una herramienta de C# denominada Rubeus para el robo de credenciales, lo que en última instancia permite que el atacante se mueva lateralmente a un servidor de Windows con privilegios de administrador de dominio.

Después, los permisos elevados se arman para organizar un ataque DCSync, lo que permite que el atacante simule el comportamiento de un controlador de dominio (DC) y recupere las credenciales de otros controladores de dominio.

Otras herramientas utilizadas como parte del ataque incluyen una utilidad legítima llamada netscan.exe para escanear la red en busca de movimiento lateral, así como el software de sincronización de archivos rclone para extraer directorios de interés para el servicio de almacenamiento en la nube de MEGA.

Los hallazgos surgen cuando los investigadores de Team Cymru arrojaron más luz sobre el protocolo BackConnect (BC) usado por IceID para ofrecer una funcionalidad adicional después del compromiso, incluido un módulo VNC que proporciona un canal de acceso remoto.

«En el caso de BC, parece que hay dos operadores que administran el proceso general con roles distintos», dijeron los investigadores, agregando que *«gran parte de la actividad ocurre durante la semana laboral típica».*

El desarrollo también sigue a un informe de Proofpoint en noviembre de 2022 de que un resurgimiento en la actividad de Emotet se ha relacionado con la distribución de una nueva versión de IceID.