Se ha estado observando a atacantes que están abusando del software de simulación de adversarios legítimos en sus ataques, en un intento de pasar desapercibidos y evadir la detección.

Unit 42 de Palo Alto Networks, dijo que una muestra de malware cargada en la base de datos VirusTotal el 19 de mayo de 2022 contenía una carga útil asociada con Brute Ratel C4, un kit de herramientas sofisticado relativamente nuevo *«diseñado para evitar la detección y respuesta de punto final (EDR) y capacidades antivirus (AV)».*

Escrito por un investigador de seguridad indio llamado Chetan Nayak, Brute Ratel (BRc4) es análogo a Cobalt Strike y se describe como *«un centro de comando y control personalizado para el equipo rojo y la simulación del adversario».*

El software comercial se lanzó por primera vez a fines de 2020 y desde entonces ha obtenido más de 480 licencias en 350 clientes. Cada licencia se ofrece a 2500 dólares por usuario durante un año, luego de lo cual, se puede renovar por la misma duración al costo de 2250 dólares.

BRc4 está equipado con una gran variedad de características como la inyección de procesos, la automatización de los TTP adversarios, la toma de capturas de pantalla, carga y descarga de archivos, compatibilidad con múltiples canales de comando y control y la capacidad de mantener ocultos los artefactos de memoria de los motores antimalware, entre otros.

Al igual que Cobalt Strike, Brute Ratel también permite implementar 'Badgers' en hosts comprometidos que pueden albergar un servidor controlador de atacante para recibir comandos de la siguiente etapa o filtrar datos.

El artefacto, que se cargó desde Sri Lanka, se hace pasar por el curriculum vitae de un individuo llamado Rosahn Bandara («Roshan_CV.iso»), pero en realidad es un archivo de imagen de disco óptico que, al ejecutarlo, se monta como una unidad de Windows que contiene un documento de Word aparentemente inofensivo que, al iniciarse, instala BRc4 en la máquina del usuario y establece comunicaciones con un servidor remoto.

La entrega de archivos ISO empaquetados generalmente se logra por medio de campañas de correo electrónico de phishing, aunque no está claro si se utilizó el mismo método para entregar la carga útil al entorno de destino.

«La composición del arhivo ISO, Roshan_CV.ISO, se parece mucho a la de otras piezas APT de estados nacionales», dijeron los investigadores de Unit 42, Mike Harbison y Peter Renals, señalando similitudes con la de un archivo ISO empaquetado previamente atribuido a la nación rusa, específicamente al actor estatal APT29.

APT29 saltó a la fama el año pasado luego de que se culpara al grupo patrocinado por el estado de orquestar un ataque cibernético a la cadena de suministro de SolarWinds.

La compañía de seguridad cibernética dijo también que detectó una segunda muestra que se cargó a VirusTotal desde Ucrania un día después y que mostraba superposiciones de código con el de un módulo responsable de cargar BRc4 en la memoria. Desde entonces, la investigación ha descubierto siete muestras más de BRc4 que datan de febrero de 2021.

Eso no es todo. Al examinar el servidor de comando y control que se utilizó como canal encubierto, se identificaron varias víctimas potenciales. Esto incluye una organización argentina, un proveedor de televisión IP que proporciona contenido de América del Norte y del Sur y un importante fabricante textil en México.

> *«La aparición de una nueva prueba de penetración y capacidad de emulación de adversarios es significativa. Aún más alarmante es la efectividad de BRc4 para derrotar las modernas capacidades defensivas de detección EDR y AV»,* agregaron los investigadores.

Poco después de que los hallazgos se hicieran públicos, Nayak escribió en Twitter que *«se*

tomaron las medidas adecuadas contra las licencias encontradas que se vendieron en el mercado negro», agregando que BRc4 v1.1 *«cambiará todos los aspectos de IoC encontrados en las versiones anteriores».*