Investigadores de seguridad cibernética están alertando sobre una nueva cepa de ransomware llamada DarkRadiation, que se implementó completamente en Bash y apunta a los contenedores en la nube de Linux y Docker, mientras confían en el servicio de mensajería Telegram para comunicaciones de comando y control (C2).

> *«El ransomware está escrito en script Bash y apunta a distribuciones Red Hat/Cent OS y Debian Linux. El malware usa el algoritmo AES de OpenSSL con modo CBC para cifrar archivos en distintos directorios. También usa la API de Telegram para enviar un estado de infección a los actores de la amenaza»,* dijeron los investigadores de Trend Micro.

Hasta ahora, no hay información disponible sobre los métodos de entrega o evidencia de que el ransomware ya se haya implementado en ataques en la naturaleza.

Los hallazgos provienen de un análisis de una colección de herramientas de piratería alojados en la infraestructura del actor de amenazas no identificado (dirección IP «185.141.25.168») en un directorio llamado «*api_attack*». El conjunto de herramientas fue notado por primera vez por el usuario de Twitter @r3dbU7z el 28 de mayo.

La cadena de infección de DarkRadiation implica un proceso de ataque de varias etapas y es notable por su amplia dependencia de los scripts Bash para recuperar el malware y cifrar los archivos, así como la API de Telegram para comunicarse con el servidor C2 a través de claves API codificadas.

El ransomware, que al parecer está en desarrollo activo, aprovecha las tácticas de ofuscación para codificar el script Bash utilizando una herramienta de código abierto llamada «node-bash-ofuscate» para dividir el código en varios fragmentos, seguido de asignar un nombre de variable a cada segmento y reemplazar el script original con referencias variables.

Después de la ejecución, DarkRadiation comprueba si se ejecuta como usuario root, y de ser así, utiliza los permisos elevados para descargar e instalar las bibliotecas Wget, cURL y

OpenSSL, y toma una captura periódica de los usuarios que actualmente están conectados a un sistema informático Unix, usando el comando «who» cada cinco segundos, cuyos resultados se exfiltran a un servidor controlado por el atacante usando la API de Telegram.

> *«Si alguno de estos no está disponible en el dispositivo afectado, el malware intenta descargar las herramientas necesarias usando YUM (Yellowdog Updater, Modified), un administrador de paquetes basado en Python ampliamente adoptado por distribuciones populares en Linux como Red Hat y CentOS»,* dijeron los investigadores de SentinelOne.

El ransomware en su fase final de la infección, recupera una lista de todos los usuarios disponibles en el sistema comprometido, sobrescribe las contraseñas de usuarios existentes con *«megapassword»* y elimina todos los usuarios de shell, pero no antes de crear un nuevo usuario con el nombre *«ferrum»* y contraseña *«MegPw0rD3»* para seguir con el proceso de cifrado.

El análisis de SentinelOne revela diferentes variaciones en las que la contraseña del usuario ferrum se descarga del servidor C2 del atacante en pocas versiones, mientras que en otras está codificada con cadenas como «*$MeGaPass123#*«, lo que implica que el malware está sufriendo cambios rápidos antes de la implementación real.

> *«Debe tenerse en cuenta que el ransomware agrega símbolos radiactivos (.☢) como una extensión de archivo para un archivo cifrado»,* dijo el investigador de amenazas de Trend Micro, Aliakbr Zahravi.

Una segunda parte móvil asociada con el ataque es un gusano SSH que está diseñado para recibir una configuración de credenciales en forma de un parámetro codificado en base64. Posteriormente, este argumento codificado se utiliza para conectarse al sistema de destino mediante el protocolo SSH y, finalmente, descargar y ejecutar el ransomware.

Además de informar el estado de ejecución, junto con la clave de cifrado, al canal de Telegram del adversario a través de la API, DarkRadiation también cuenta con capacidades para detener y deshabilitar todos los contenedores Docker en ejecución en la máquina infectada, después de lo cual se muestra una nota de rescate para el usuario.

> *«El malware escrito en lenguajes de scripts de shell permite a los atacantes ser más versátiles y evitar algunos métodos de detección comunes»,* dijeron los investigadores de SentinelOne.
>
> *«Como no es necesario volver a compilar los scripts, se pueden iterar más rápidamente. Además, debido a que algunos software de seguridad se basan en firmas de archivos estáticos, estos se pueden eludir fácilmente mediante una iteración rápida y el uso de herramientas simples de ofuscador para generar un script completamente diferente».*