El grupo de cryptojacking rastreado como 8220 Gang, fue visto usando como arma una vulnerabilidad de seis años en los servidores Oracle WebLogic para atrapar instancias vulnerables en una red de bots y distribuir malware de minería de critpomonedas.

La vulnerabilidad en cuestión es CVE-2017-3506 (puntaje CVSS: 7.4), que, al ser explotada con éxito, podría permitir que un atacante no autenticado ejecute comandos arbitrarios de forma remota.

> *«Esto permite a los atacantes obtener acceso no autorizado a datos confidenciales o comprometer todo el sistema»,* dijo el investigador de Trend Micro, Sunil Bharti.

8220 Gang, documentado por primera vez por Cisco Talos a finales de 2018, recibe ese nombre por su uso original del puerto 8220 para comunicaciones de red de comando y control (C2).

> *«8220 Gang identiifca objetivos mediante el escaneo de hosts mal configurados o vulnerables en la Internet pública. Se sabe que 8220 Gang hace uso de ataques de fuerza bruta SSH después de la infección con el fin de moverse lateralmente dentro de una red comprometida»*, dijo SentinelOne el año pasado.

A inicios de este año, Sydig detalló los ataques montados por el grupo de crimeware de «baja habilidad» entre noviembre de 2022 y enero de 2023, que tienen como objetivo violar los servidores web vulnerables Oracle WebLogic y Apache, así como implementar un minero de criptomonedas.

También se ha observado que hace uso de un descargador de malware estándar conocido

como PureCrypter, así como un encriptador con nombre en código ScrubCrypt para ocultar la carga útil del minero y evadir la detección por parte del software de seguridad.

En la última cadena de ataques documentada por Trend Micro, la vulnerabilidad de Oracle WebLogic Server se aprovecha para entregar una carga útil de PowerShell, que después se utiliza para crear otro script de PowerShell ofuscado en la memoria.

Esta secuencia de comandos de PowerShell recién creada desactiva la detección de la interfaz de análisis antimalware de Windows (AMSI) e inicia un binario de Windows que posteriormente llega a un servidor remoto para recuperar una carga útil «meticulosamente ofuscada».

El archivo DLL intermedio, por su parte, está configurado para descargar un minero de criptomonedas desde uno de los tres servidores C2: 179.43.155[.]202, work.letmaker[.]top y su-94.letmaker[.]top, usando los puertos TCP 9090, 9091 o 9092.

Trend Micro dijo que los ataques recientes también implicaron el uso indebido de una herramienta legítima de Linux llamada lwp-download para guardar archivos arbitrarios en el host comprometido.

> *«lwp-download es una utilidad de Linux presente en varias plataformas de forma predeterminada, y 8220 Gang hace que esto sea parte de cualquier rutina de malware que puede afectar a una serie de servicios, incluso si se reutiliza más de una vez»,* dijo Bharti.

> *«Teniendo en cuenta la tendencia del actor de amenazas a reutilizar herramientas para distintas campañas y abusar de herramientas legítimas como parte del arsenal, los equipos de seguridad de las organizaciones podrían verse desafiados a encontrar otras solucionas de detección y bloqueo para defenderse de los ataques que abusan de esta utilidad».*