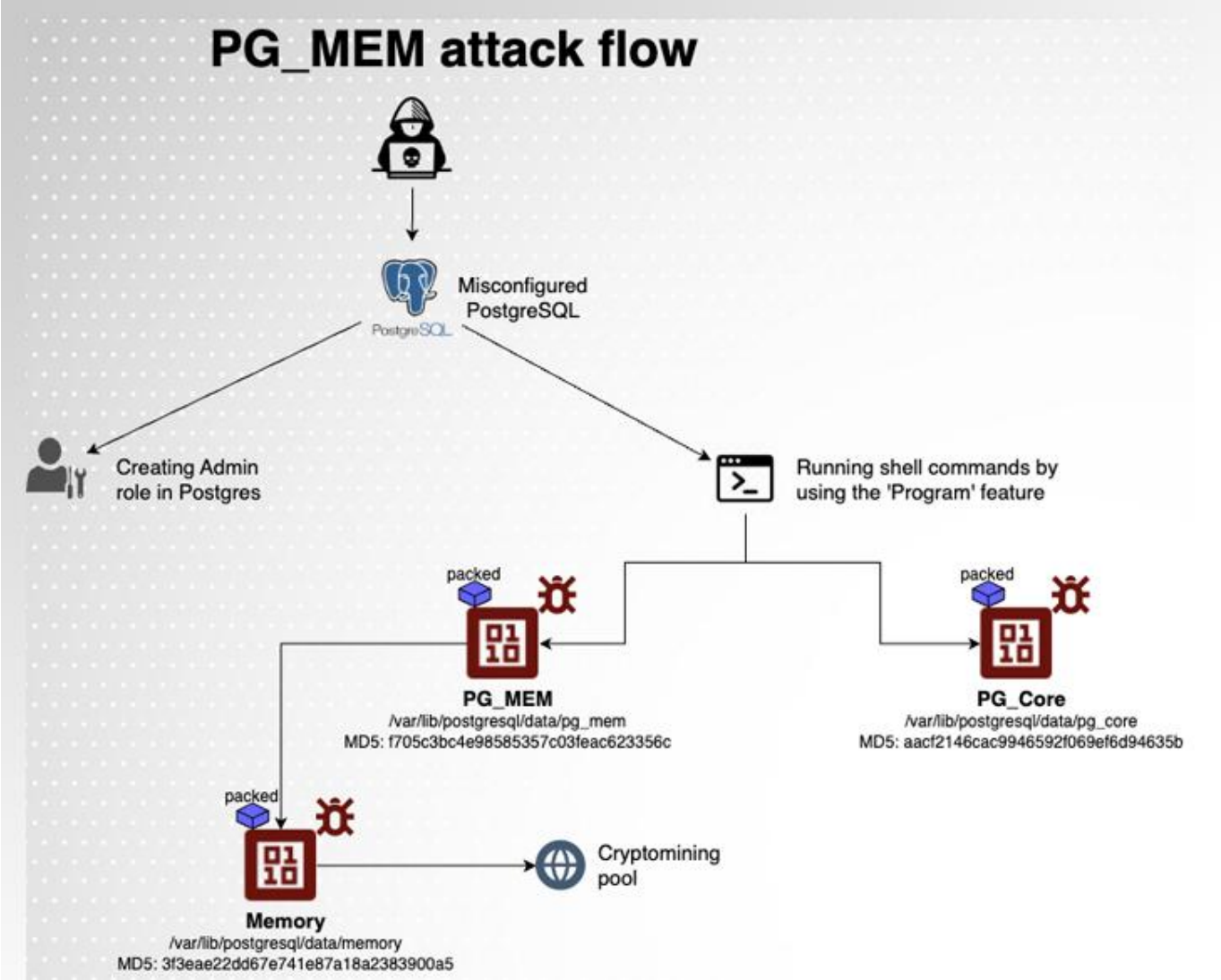
Investigadores en ciberseguridad han identificado una nueva cepa de malware llamada PG_MEM, diseñada para minar criptomonedas después de realizar ataques de fuerza bruta en instancias de bases de datos PostgreSQL.

> *«Los ataques de fuerza bruta en Postgres consisten en intentar adivinar repetidamente las credenciales de la base de datos hasta obtener acceso, aprovechando contraseñas débiles»*, explicó Assaf Morag, investigador de seguridad en Aqua, en un informe técnico.
>
> *«Una vez que se logra el acceso, los atacantes pueden utilizar el comando SQL `COPY ... FROM PROGRAM` para ejecutar comandos shell arbitrarios en el host, lo que les permite llevar a cabo actividades maliciosas como el robo de datos o la instalación de malware».*

La cadena de ataque observada por la firma de seguridad en la nube implica dirigirse a bases de datos PostgreSQL mal configuradas para crear un rol de administrador en Postgres y aprovechar una función llamada PROGRAM para ejecutar comandos shell.

Además, después de un ataque de fuerza bruta exitoso, el atacante lleva a cabo un reconocimiento inicial y ejecuta comandos para despojar al usuario «postgres» de sus privilegios de superusuario, restringiendo así las capacidades de otros posibles atacantes que pudieran obtener acceso de la misma manera.



Los comandos shell descargan dos cargas útiles desde un servidor remoto («128.199.77[.]96»), conocidas como PG_MEM y PG_CORE, que tienen la capacidad de terminar procesos competidores (como Kinsing), establecer persistencia en el host y, finalmente, desplegar un minero de criptomonedas Monero.

Esto se consigue utilizando un comando de PostgreSQL llamado COPY, que permite transferir datos entre un archivo y una tabla de la base de datos. En particular, explota un parámetro conocido como PROGRAM, que permite al servidor ejecutar el comando indicado y guardar

los resultados de la ejecución en la tabla.

> *«Aunque el principal impacto es la minería de criptomonedas, en este punto el atacante también puede ejecutar comandos, visualizar datos y controlar el servidor»,* mencionó Morag.
>
> *«Esta campaña explota bases de datos Postgres expuestas a internet con contraseñas débiles. Muchas organizaciones conectan sus bases de datos a internet; la debilidad de la contraseña es resultado de una mala configuración y la falta de controles de identidad apropiados».*

Esta revelación coincide con un informe de los Laboratorios de Seguridad de Datadog, que describe una campaña de ataque oportunista que aprovecha la vulnerabilidad Log4Shell (CVE-2021-44228, puntaje CVSS: 10.0) en Apache Log4j para descargar un script bash ofuscado, capaz de recopilar información del sistema, desplegar un minero XMRig y un shell reverso para acceso remoto.