BOLETIM DE SEGURANÇA

Malware PG_MEM ataca bancos de dados PostgreSQL para mineração de criptomoedas

heimdall
security research
A DIVISION OF ISH

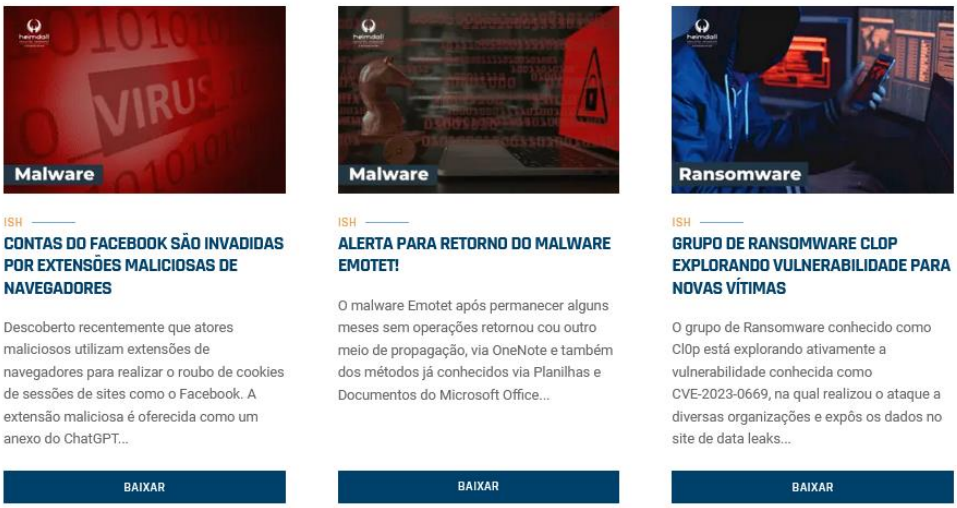
TLP: CLEAR

Receba alertas e informações sobre segurança cibernética e ameaças rapidamente, por meio do nosso **X**.

[Heimdall Security Research]

Acesse boletins diários sobre agentes de ameaças, *malwares*, indicadores de comprometimentos, TTPs e outras informações no *site* da ISH.

[Boletins de Segurança – Heimdall]



SUMÁRIO

LISTA DE TABELAS

LISTA DE FIGURAS

1 SUMÁRIO EXECUTIVO

Pesquisadores de segurança identificaram o ***PG_MEM***, um novo malware que compromete bancos de dados **PostgreSQL** através de ataques de força bruta. Após ganhar acesso, o malware entrega payloads para ocultar suas atividades e minera criptomoedas.

2 INFORMAÇÕES SOBRE A AMEAÇA

Um ataque de força bruta bem-sucedido foi observado em um banco de dados PostgreSQL, explorando uma vulnerabilidade que permite a execução de comandos. O invasor criou uma função de superusuário e deixou dois arquivos no disco, usados para eliminar concorrentes, evitar detecção, manter persistência e implantar mineradores de criptomoedas. Além disso, o invasor pode executar comandos, visualizar dados e controlar o servidor.

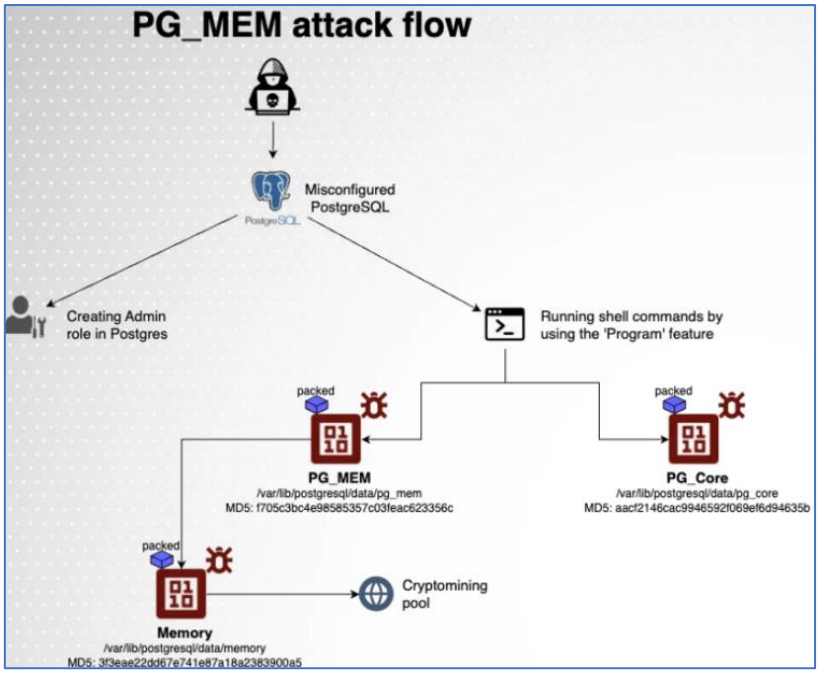


Figura 1 – Fluxo de ataque do PG_MEM.

O ataque começou com várias tentativas de login no banco de dados PostgreSQL sendo recusadas até que o invasor adivinhou corretamente o nome de usuário e a senha do honeypot, que foram configurados para serem facilmente adivinhados. Após o sucesso na adivinhação, a sequência de ataque foi iniciada com a execução de um conjunto de comandos SQL.

```
CREATE ROLE pgsql_user WITH LOGIN SUPERUSER PASSWORD 'b371823c6a5bab4b0ff8c3de6f8a1cc8';
SELECT current user;
SELECT username,usesuper FROM pg_catalog.pg_user;
ALTER user "postgres" with nosuperuser;
```

Figura 2 – Comando do agente de ameaça para criar um novo superusuário (backdoor).

O agente de ameaça começa criando uma nova função de usuário com permissões de login e privilégios elevados. Em seguida, ele interage com o usuário que inicialmente permitiu o acesso ao sistema. O comando SELECT CURRENT_USER é usado para obter o nome do usuário atual na sessão do banco de dados.

O próximo comando lista os nomes dos usuários e verifica se possuem privilégios de superusuário. Posteriormente, o usuário postgres é removido dos privilégios de superusuário, limitando assim os privilégios de outros agentes que possam acessar o sistema através de uma senha fraca.

O agente de ameaça está coletando informações detalhadas sobre o sistema.

```
SHOW hba_file;
SELECT version();
CREATE TABLE IF NOT EXISTS pg_temp.log_tmp(filename TEXT);
TRUNCATE pg_temp.log_tmp;
COPY pg_temp.log_tmp FROM PROGRAM 'uname -m 2>&1 || exit 0' WITH DELIMITER '~';
SELECT * FROM pg_temp.log_tmp;
TRUNCATE pg_temp.log_tmp; (repeated multiple times)
COPY pg_temp.log_tmp FROM PROGRAM 'uname -r 2>&1 || exit 0' WITH DELIMITER '~';
COPY pg_temp.log_tmp FROM PROGRAM 'whoami 2>&1 || exit 0' WITH DELIMITER '~';
```

Figura 3 – Compilação de comandos destinados a descobrir o sistema.

Utilizando o Shodan, um mecanismo de busca especializado em dispositivos conectados à Internet, foi possível identificar bancos de dados PostgreSQL possivelmente vulneráveis. Ao pesquisar no Shodan por instâncias de Postgres acessíveis publicamente, foi encontrado mais de 800.000 bancos de dados expostos na Internet. Esse número alarmante ressalta a importância urgente de proteger servidores de banco de dados contra ataques de força bruta e possíveis explorações.

Figura 4 – Resultados no Shodan da busca por servidores Postgres voltados para a Internet.

3 MITRE ATT&CK - TTPs

Tática	Técnica	Detalhes
Initial Access	T1190	Consiste em técnicas que usam vários vetores de entrada para ganhar sua posição inicial dentro de uma rede.
Execution	T1059.004	Consiste em técnicas que resultam em código controlado pelo adversário em execução em um sistema local ou remoto.
Persistence	T1136.001 T1098 T1053.003	Consiste em técnicas que os adversários usam para manter o acesso aos sistemas em reinicializações, credenciais alteradas e outras interrupções que podem cortar seu acesso.
Privilege scalation	T1068	Consiste em técnicas que os adversários usam para obter permissões de nível mais alto em um sistema ou rede.
Defense Evasion	T1070.004 T1036.004	Consiste em técnicas que os adversários usam para evitar a detecção durante seu comprometimento.
Credentials Access	T1110.002	Consiste em técnicas para roubar credenciais como nomes de contas e senhas. Técnicas usadas para obter credenciais incluem keylogging ou credential dumping.
Discovery	T1082 T1057	Consiste em técnicas que um adversário pode usar para obter conhecimento sobre o sistema e a rede interna.
Collection	T1005	Consiste em técnicas que os adversários podem usar para reunir informações e as fontes de onde as informações são coletadas que são relevantes para seguir os objetivos do adversário.
Command and Control	T1105 T1071.001	Consiste em técnicas que adversários podem usar para se comunicar com sistemas sob seu controle dentro de uma rede de vítima.
Impact	T1496	Consiste em técnicas que os adversários usam para interromper a disponibilidade ou comprometer a integridade ao manipular processos comerciais e operacionais.

Tabela 1 – Tabela MITRE ATT&CK.

4 RECOMENDAÇÕES

Além dos indicadores de comprometimento elencados abaixo pela ISH, poderão ser adotadas medidas visando a mitigação da infecção do referido *malware*, como por exemplo:

Utilização de senhas fortes

- Utilize senhas complexas para evitar ataques de força bruta.

Controle de acesso

- Restrinja o acesso aos servidores PostgreSQL usando firewalls e listas de controle.

Monitoramento contínuo

- Implemente monitoramento para detectar atividades suspeitas.

Atualizações regulares

- Mantenha o PostgreSQL e outros softwares atualizados.

Proteção em tempo real

- Utilize ferramentas de proteção em tempo real para detectar e mitigar atividades maliciosas.

5 INDICADORES DE COMPROMISSOS

A ISH Tecnologia realiza o tratamento de diversos indicadores de compromissos coletados por meio de fontes abertas, fechadas e também de análises realizadas pela equipe de segurança Heimdall. Diante disto, abaixo listamos todos os Indicadores de Compromissos (IOCs) relacionadas a análise do(s) artefato(s) deste relatório.

Indicadores de compromisso do artefato	
md5:	3f3eae22dd67e741e87a18a2383900a5
sha1:	b0c796a420461d73a1709f7fced40b55fcf6c27f
sha256:	4140445930daa6271d1cac4fe9be8dbbfcefeab3cc6b84fd06dba98c6571b280
File name:	memory

Indicadores de compromisso do artefato	
md5:	aacf2146cac9946592f069ef6d94635b
sha1:	85198288e2ff1dad718cd84876a0b0d3173a641e
sha256:	551d4df1d525b68ee354fcee133a505857aff4b5041e1fe657d8813ba5303b2d
File name:	pg_core2

Indicadores de compromisso do artefato	
md5:	f705c3bc4e98585357c03feac623356c
sha1:	d761738d2cf25fc9813c715dc142e93697f2e4b9
sha256:	c410768b1ba5bacaf60f5f32aa7672765c2f2f4e41b10c75770e6df9eba5f765
File name:	pg_mem.bin

Tabela 2 – Indicadores de Compromissos de artefatos

6 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **Aquasec**
- **Thehackernews**

7 AUTORES

- **Leonardo Oliveira Silva**

heimdall
security research
A DIVISION OF ISH