Ameaças atores explorando servidores MS-SQL para implantar a estrutura

Data: 2025-09-30 09:19:32

Autor: Inteligência Against Invaders

Um aumento nos ataques direcionados aos servidores MS-SQL gerenciados indevidamente,

culminando na implantação da estrutura de comando e controle de código aberto XIEBROC2 (C2).

Em funcionalidade semelhante a ferramentas legítimas como o cobalto, o Xiebroc2 oferece recursos para coleta de informações, controle remoto e evasão de defesa, tornando-a uma opção atraente para atores de ameaças que buscam uma plataforma de intrusão econômica.

Em um incidente confirmado, os invasores alavancaram publicamente as credenciais do MS-SQL Server para obter acesso não autorizado.

Depois de forças de contas fracas ou padrão, os intrusos executaram uma sequência de implantações de carga útil comuns aos compromissos do MS-SQL, com os mineradores de criptomoeda sendo o malware principal de escolha.

Uma vez autenticado, os atores de ameaças abandonaram a Juicypotato, um utilitário de escalonamento de privilégio que explora privilégios específicos do Windows dentro dos tokens do processo MS-SQL em execução.

Os pesquisadores do Ahnlab Security Intelligence Center (ASEC) têm descoberto Um serviço do SQL Server opera sob uma conta de baixa privilégio por padrão, a Juicypotato permitiu que os atacantes elevassem os privilégios do sistema.

A evidência do download e da execução foi capturada nos logs do servidor, mostrando a função Invoke-WebRequest do PowerShell, puxando a carga útil do XIEBROC2 sobre o HTTP. Essa sequência ressalta o risco crítico representado por servidores de banco de dados acessíveis ao público sem políticas de credenciais robustas ou controles de acesso em nível de rede.

Com os privilégios do sistema protegidos, os atacantes executaram um comando PowerShell para recuperar e instalar o XIEBROC2 diretamente de seu Github repositório.

XIEBROC2 Framework

O componente de implante do Xiebroc2-a funcionalidade principal da backdoor-está escrita em Go, fornecendo suporte de plataforma cruzada para Windows, Linux e sistemas macos.

Uma vez implantado, o implante inicia uma conexão com o servidor C2 do atacante, autentica usando uma chave AES pré -configurada e aguarda comandos. Os recursos comuns incluem:

- Acesso à casca reversa.

- Gerenciamento de arquivos e processos.
- Monitoramento de rede e captura de pacotes.
- Tunelamento de proxy reverso.
- Captura de captura de tela.

Após a execução, o XIEBROC2 coleta detalhes do ambiente, como ID do processo (PID), ID de hardware (HWID), nome do computador e nome de usuário e, em seguida, se conecta transparentemente ao Servidor C2 para registrar o host comprometido. No incidente monitorado pela ASEC, os parâmetros de configuração foram os seguintes:

- Hostport: 1.94.185[.]235: 8433.
- Protocolo: sessão/reverse_ws.
- ListerName: Test2.
- Aeskey: qwert_csdmahuatw.

Esses valores permitiram ao implante estabelecer uma sessão de Websocket criptografada persistente sobre o TCP, fornecendo comunicação bidirecional resiliente mesmo na presença de interrupções da rede.

Depois de conectado, o invasor pode executar comandos arbitrários ou implantar cargas úteis adicionais, cimentando o ponto de apoio para um movimento lateral ou exfiltração lateral.

Mitigações

Aplicar fortes políticas de autenticação: Os administradores devem desativar credenciais fracas ou padrão nos servidores MS-SQL. Implementar senhas complexas e exclusivas e ativar as políticas de bloqueio de conta reduzirão drasticamente a taxa de sucesso de força bruta e ataques de dicionário.

Limite a exposição pública: As instâncias MS-SQL não devem estar diretamente acessíveis na Internet. Empregue regras de segmentação de rede e firewall para restringir o acesso ao banco de dados a apenas servidores de aplicativos autorizados ou pontos de extremidade da VPN.

Patch e atualização: Verifique se todos os pontos de extremidade executando os serviços MS-SQL estão totalmente corrigidos e executando as atualizações de segurança mais recentes. As vulnerabilidades nos processos de hospedagem de serviço podem facilitar o compromisso inicial e a escalada de privilégios.

Monitore e alerta: Implante sistemas de detecção de intrusão capazes de sinalizar tentativas de login anômalos, execução inesperada da ferramenta de escalonamento de privilégio (por exemplo, Juicypotato) e conexões de rede de saída incomuns-especialmente para endereços IP externos desconhecidos e portas incomuns.

Proteção de terminais: Utilize soluções antimalware atualizadas para detectar e quarentena ferramentas conhecidas como componentes da estrutura Juicypotato e C2. A análise comportamental pode fornecer alerta precoce das atividades de reconhecimento ou movimento lateral.

A ASEC continua a monitorar ameaças emergentes direcionando servidores de banco de dados e insta as organizações a adotar uma abordagem em profundidade.

A falha em garantir mecanismos de autenticação, manter patches atualizados e restringir o acesso à rede pode levar a infecções repetidas e comprometer a infraestrutura crítica. Hoje, a ação preventiva protege as estruturas de intrusão avançadas de amanhã.

Siga -nos Google News**Assim,**LinkedIn**e**X**Para obter atualizações instantâneas e definir GBH como uma fonte preferida em**Google**.**