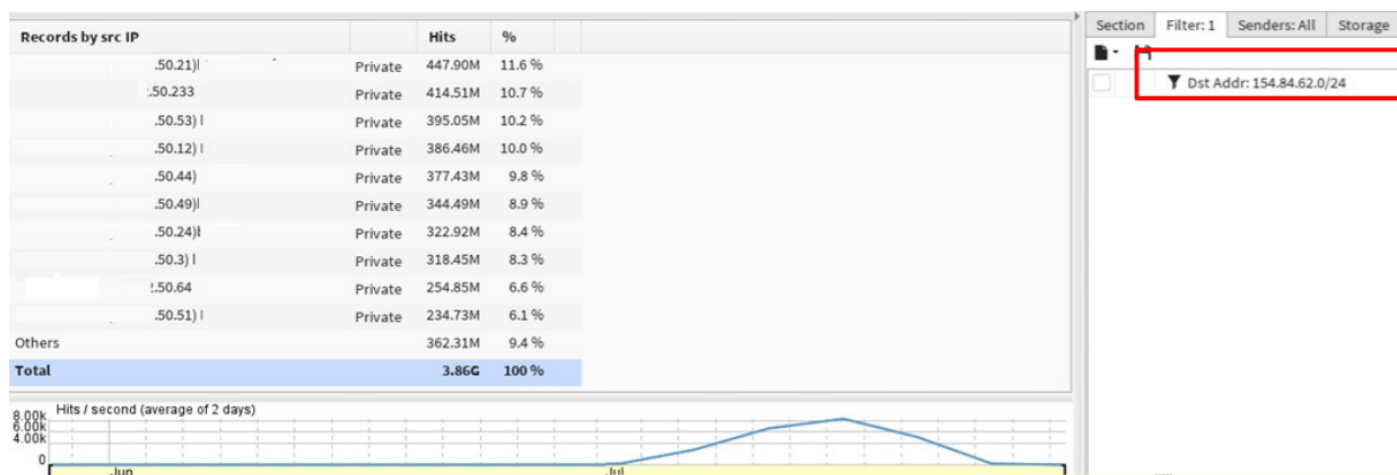


Medidas de contenção em caso de ocorrência

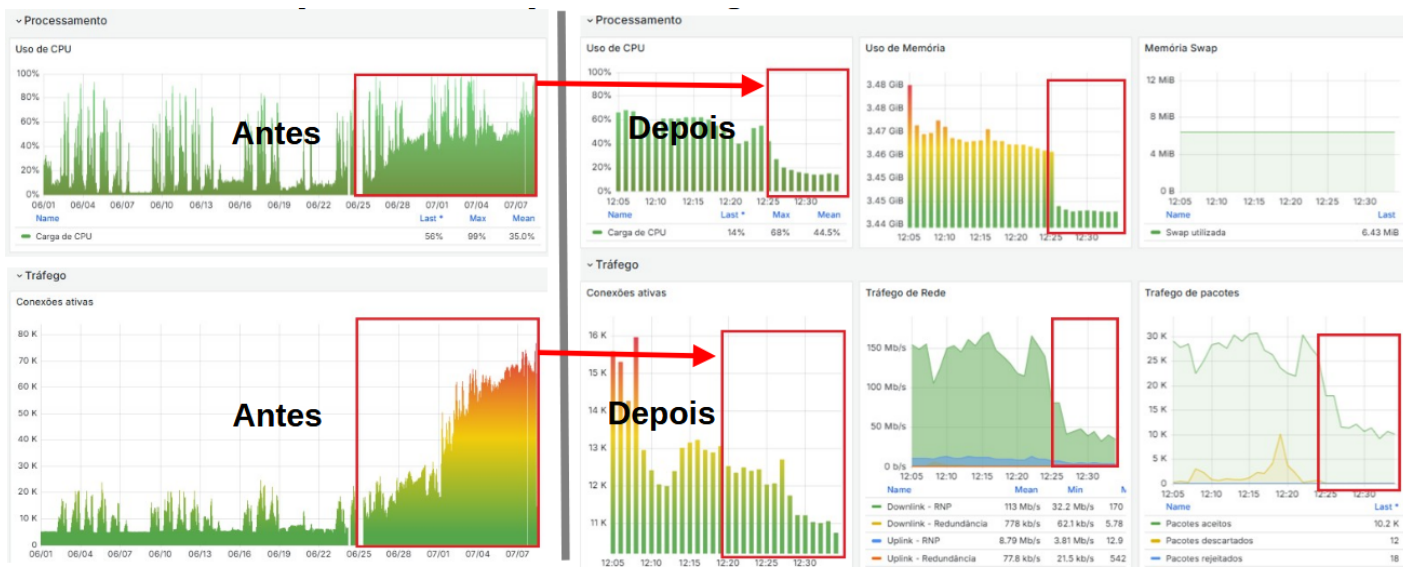
Ainda é preciso buscar tentativas de evasão do malware na rede. Sim, malwares possuem inteligência em seu código, suficiente para trocar seus servidores de comandos e controle mediante a suspeita e/ou bloqueios. Estes métodos são chamados de **TÉCNICAS DE EVASÃO**:

Assim, utilizando o endereço CIDR completo, que nos foi retornado pela plataforma VirusTotal, ampliamos nossa análise, e outros dispositivos, que não foram identificados inicialmente, passam a ser identificados como comprometidos, se comunicando com tais servidores de comando e controle maliciosos.



Ações de contenção:

Remoção física e virtual imediata de todos os dispositivos e suas interfaces de rede vinculadas a este tráfego. Mesmo dispositivos que não sejam TvBox, podem ter sido comprometidos pelo malware, através da exploração de vulnerabilidades para se deslocar na rede. O impacto positivo sobre a qualidade e quantidade da rede é imediato:



Imediata desconexão/isolamento do segmento de rede onde o incidente foi detectado, evitando contato com as demais redes.

Bloqueio local vertical (entrada e saída para internet) e horizontal (redes internas) dos ranges de IPs externos envolvidos no incidente.

Revisão completa de todas as regras de segmentação entre vlans, recriando-as e incluindo a microsegmentação por origem, destino, serviço, porta e protocolo.

Recriação do ZERO de todos os serviços afetados (que não sejam TvBox), através de instalações íntegras. TvBox devem permanecer fora da rede (em casos de estudos acadêmicos, devem ser usadas redes totalmente segmentadas, sem contatos com as demais redes, em caso de impossibilidade, tais dispositivos não devem ser utilizados).

Atualização de todos os serviços e appliances da rede, mesmo os que não afetados pelo incidente;

ATENÇÃO REDOBRADA AO MONITORAMENTO DE REDE E DE ACESSOS.

Revision #9

Created 2025-12-08 16:41:56 -03 by Ado Cardoso da Silva

Updated 2025-12-11 09:21:33 -03 by Ado Cardoso da Silva