Security Snares

# RansomSnare™

## Interrompa o Ransomware na Primeira Tentativa. Antes que ele Criptografe Qualquer Arquivo.

Com a proliferação de novas variantes e famílias de ransomware e vulnerabilidades exploráveis, as ferramentas tradicionais de segurança de endpoint e anti-malware enfrentam uma tarefa cada vez mais difícil para impedir que o ransomware entre na rede. A necessidade constante de atualizações e patches de correção — para corrigir falhas e obter as assinaturas mais recentes — ajuda também a explicar por que o ransomware se espalhou com tanta rapidez, especialmente diante de uma força de trabalho cada vez mais móvel. A chave não é abandonar sua ferramenta atual de proteção de endpoint, mas sim reforçá-la, adicionando uma camada extra de proteção.

Todas as formas de ransomware têm algo em comum: ***todas precisam criptografar arquivos***. O **RansomSnare** **impede que o ransomware funcione suspendendo o processo assim que ele tenta criptografar o primeiro arquivo**.

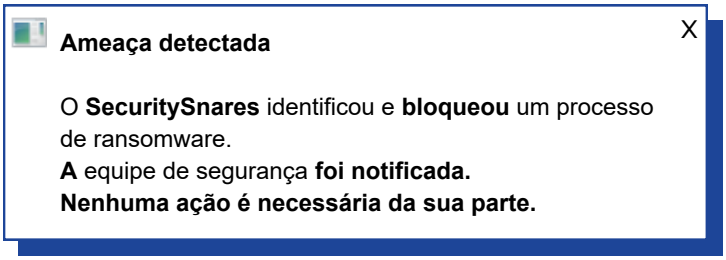
Por atuar no primeiro arquivo, o **RansomSnare** não precisa reservar blocos de espaço para "rollback" (restauração de arquivos) como outras soluções. Além disso, por ser extremamente eficiente, ele consome recursos quase imperceptíveis, causando impacto mínimo no ambiente, diferentemente das soluções baseadas em detecção comportamental.

O **RansomSnare** opera sem precisar de uma referência de sistema saudável, oferecendo defesa contínua mesmo após a restauração do ambiente após um eventual ataque. E faz tudo isso sem utilizar assinaturas, funcionando mesmo desconectado e sem necessidade de atualizações no core tecnológico.

De fato, a mesma tecnologia já interrompeu todas as formas conhecidas de ransomware nos últimos dois anos — sem depender de atualizações. — um fator crítico para equipes que trabalham remotamente.

### Como Funciona

Quando um ransomware entra no seu dispositivo, ele tenta criptografar arquivos. Neste momento em que a criptografia é tentada no primeiro arquivo, o **RansomSnare** (1) interrompe o processo, (2) alerta o usuário e (3) envia as informações para a equipe de segurança.

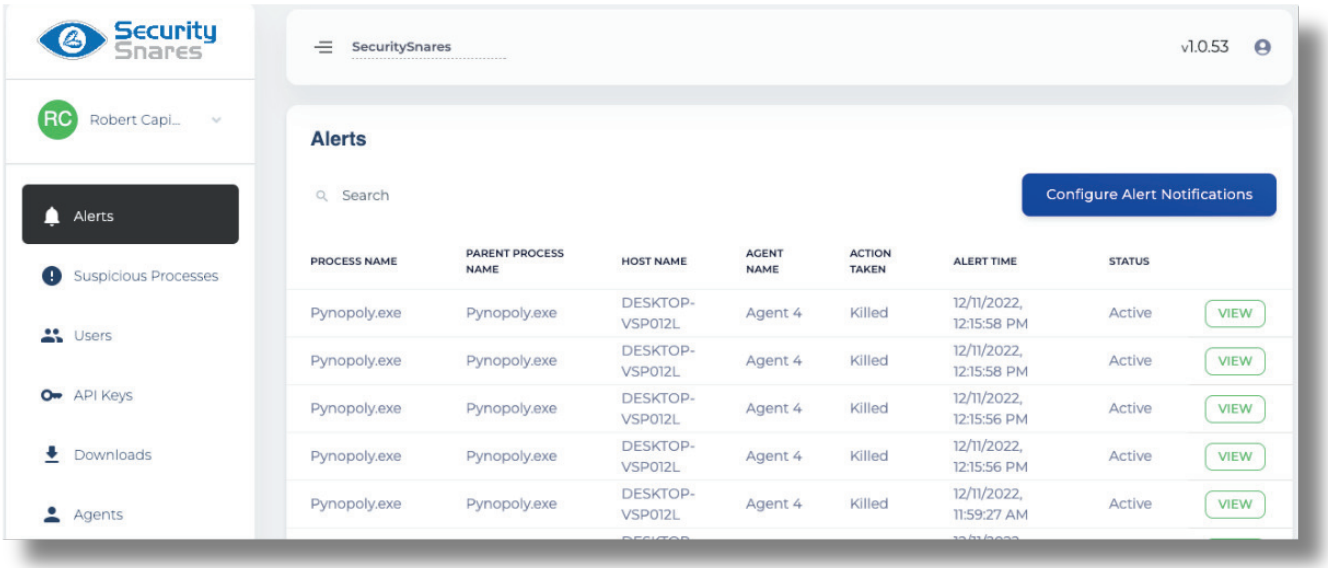



continua na próxima página

Pare o ransomware no exato instante em que ele tenta iniciar a criptografia do primeiro arquivo.

Essas informações são exibidas por meio de um console de gerenciamento, que agrega todos os endpoints protegidos pelo RansomSnare em toda a organização. Os dados podem, inclusive, ser enviados para a ferramenta de SIEM (Security Information and Event Management) de sua preferência.

Como o processo é interrompido instantaneamente, a equipe de segurança dispõe de tempo para investigar o incidente e responder de forma adequada.




A Massima Frog é parceiro autorizado SecuritySnares no Brasil. A Bunker Security é o distribuidor oficial exclusivo da SecuritySnares no Brasil.

MASSIMA FROG

Para conhecer mais sobre o RansomSnare em ação, entre em contato conosco pelo **contact-us@massimafrog.com** ou usando o QR code ao lado

**Saiba mais:**