Recursos de detecção de ransomware do Cisco WSA e verificação de integração da AMP

Contents

Problema

Foi feita uma consulta sobre se o Cisco Secure Web Appliance (WSA) fornece recursos específicos de assinatura ou detecção para o Triple X Ransomware. Essa pergunta também incluiu uma solicitação de esclarecimento sobre como verificar se uma integração entre a Advanced Malware Protection (AMP) e a Cisco Talos Threat Intelligence estava funcionando corretamente na plataforma WSA.

Ambiente

- Cisco Secure Web Appliance (WSA)
- Integração com proteção avançada contra malware (AMP)
- Integração da inteligência de ameaças do Cisco Talos
- Reputação da Web e filtragem de URL (WBRS)
- Mecanismos de varredura antimalware (Webroot, McAfee, Sophos)
- Visibilidade e controle de aplicativo (AVC)

Resolução

O Cisco Secure Web Appliance não conta com uma única assinatura dedicada especificamente nomeada para o Triple X Ransomware. Em vez disso, o WSA emprega uma arquitetura de segurança abrangente de várias camadas que utiliza várias técnicas de detecção para identificar e bloquear ameaças de ransomware, incluindo variantes Triple X Ransomware.

Métodos de detecção do WSA

A plataforma WSA usa estas técnicas de detecção para proteção contra ransomware:

- Algoritmos de correspondência de padrões
- Análise heurística
- Técnicas de emulação
- Proteção avançada contra malware (AMP) integrada com a inteligência de ameaças do Cisco Talos
- Reputação da Web e filtragem de URL (WBRS)
- Vários mecanismos de varredura antimalware, incluindo Webroot, McAfee e Sophos
- Visibilidade e controle de aplicativo (AVC)

Esses recursos de detecção são atualizados continuamente com novas regras implantadas a cada poucos minutos para garantir a proteção contra ameaças emergentes.

Verificação da integração da AMP e do Talos

Para confirmar se a integração entre o Advanced Malware Protection (AMP) e o Cisco Talos Threat Intelligence está funcionando corretamente no WSA, os administradores podem revisar estes logs:

Passo 1: Revisar os logs de acesso do WSA

Examine os logs de acesso no dispositivo WSA para verificar se os vereditos do AMP estão sendo aplicados aos arquivos baixados e às solicitações da Web.

Passo 2: Verificar registros do AMP

Examine os registros da AMP para confirmar se os resultados da análise de malware e os dados de inteligência de ameaças estão sendo processados.

Passo 3: Verificar Pontuações WBRS

Verifique se as pontuações do Web Reputation (WBRS) estão sendo preenchidas e se estão associadas às solicitações da Web nos logs.

Se os vereditos da AMP e as pontuações da WBRS estiverem sendo preenchidos e aplicados nos registros, isso indica que a integração da AMP e do Talos está funcionando conforme esperado e fornecendo decisões baseadas em inteligência de ameaças em tempo real.

Causa

Esta foi uma solicitação informativa sobre os recursos de detecção de ransomware dos WSAs, em vez de um problema técnico que requer solução de problemas. A consulta surgiu da necessidade de entender como o WSA protege contra variantes de ransomware específicas e verificar se as integrações de inteligência de ameaças estão funcionando corretamente.

Conteúdo relacionado

- Recursos e benefícios do Cisco Secure Web Appliance
- Serviços de inteligência de ameaças do Cisco Talos
- Especificações do Cisco Secure Web Appliance
- Suporte técnico e downloads da Cisco

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.