Hillstone Cloud-Sandbox:
Plataforma de Identificação e Detecção de Arquivo Malicioso

Malware avançado tornou-se tão sofisticado que consegue facilmente evadir soluções tradicionais de segurança, incluindo firewalls, IPS e tecnologias de antivírus. Para combater malware avançado, o Hillstone Cloud Sandbox oferece uma plataforma única de detecção de ameaça avançada que pode simular o ambiente de execução e analisar todas as atividades relacionadas a arquivos maliciosos, identificar ameaças avançadas e colaborar com soluções existentes para fornecer remediação rápida.

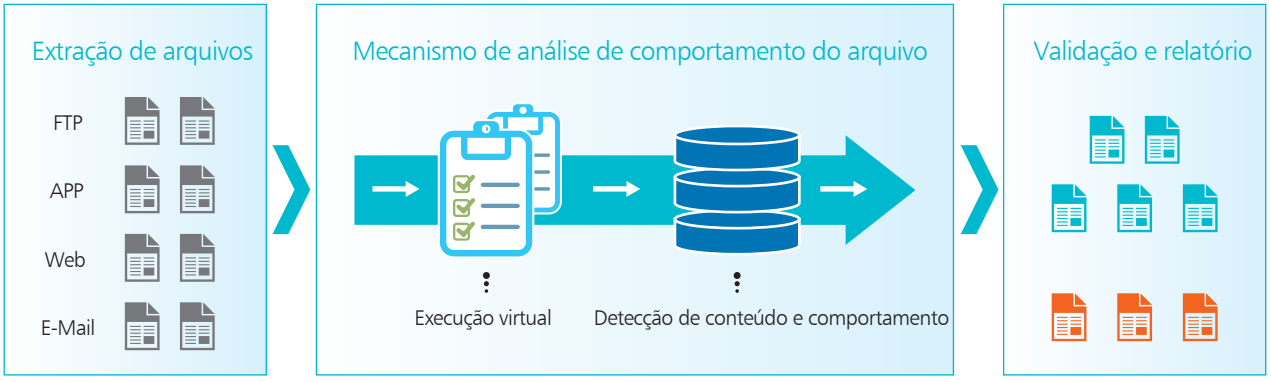

Figura 1. Hillstone Cloud-Sandbox

O Hillstone Cloud Sandbox é composto por três módulos: Análise Estática, Análise Comportamental e Inteligência de Nuvem. Os três módulos trabalham juntos para garantir a eficiência e a eficácia na detecção de arquivos maliciosos.

www.hillstonenet.br.com
Phone: 1-800-889-9860

Análise Estática: O Hillstone Cloud Sandbox faz análise estática de assinatura dos arquivos, como identificação dos tipos de arquivo, formato do arquivo e assinatura de malware conhecido. Além disso, a tecnologia de filtro frontal (por exemplo, lista de autorização de URL, validação de assinatura de arquivo, banco de dados de amostra na nuvem) pode eliminar as ameaças conhecidas para reduzir a carga de trabalho do sandbox.

Análise Comportamental: O Hillstone Cloud Sandbox pode simular vários sistemas e ambientes operacionais, e acionar comportamentos de arquivo nos ambientes simulados que se assemelham de perto a ambientes reais de produção. O Sandbox usa um modelo de aprendizagem de máquina para validar o comportamento do arquivo.

Inteligência de Nuvem: Usando informações de inteligência de ameaças compiladas globalmente a partir de nós de rede Hillstone, o Hillstone Cloud Sandbox compara as informações estáticas e o comportamento dos arquivos com as informações de inteligência, tais como assinaturas de malware, sites de phishing e nomes de domínio maliciosos, e anexa a cada arquivo uma classificação de avaliação de risco, em vez de apenas definir se ele é bom ou ruim.

Com análise estática, análise comportamental e inteligência de nuvem, o Hillstone Cloud Sandbox detecta malware com uma baixa taxa de falso-positivos e alta taxa de detecção.

Destaques do Produto

Alta taxa de detecção com análise estática e comportamental

The malware sample database on the Hillstone cloud contains more than 1 billion samples. It quickly detects whether any uploaded file matches with the malware samples. Hillstone Cloud Sandbox can simulate running environments and trigger file behaviors such as creating processes, modifying registry and requesting back chain. Unknown threats can be detected by analyzing the file behavior.

Implementação instantânea de infraestrutura de nuvem

O Hillstone Cloud Sandbox é facilmente integrado com tecnologias e soluções Hillstone, tais como Next-Generation Firewall e Hillstone CloudEdge. Ele pode ser rápida e instantaneamente implementado sem interrupção da rede.

Proteção de tráfego criptografado

Desde que a tecnologia de criptografia SSL tornou-se popular, cada vez mais aplicações usam HTTPS. Contudo, o malware atual também usa tecnologia de criptografia SSL para escapar de detecção. O Hillstone Cloud Sandbox pode decodificar o tráfego criptografado e recuperar os arquivos no tráfego criptografado. Com essa abordagem, o malware pode ser detectado, mesmo se estiver oculto no tráfego criptografado.

Medidas contra a tecnologia anti-sandbox

O Hillstone Cloud Sandbox suporta a identificação e detecção de malware anti-sandbox. Por ocultar informações de processamento de sandbox como modelo do kernel e informações de registro, o Hillstone Cloud Sandbox pode simular os ambientes operacionais. Para evitar que o malware escape de detecção, o Hillstone Cloud Sandbox simula operações manuais e interativas e assume o controle da API para que o comportamento do malware possa ser acionado.

Informações abrangentes sobre ameaça nos relatórios

Depois de detectar malware e ameaças desconhecidas, o Hillstone Cloud Sandbox exibe alarmes e notificações, bem como relatórios abrangentes de comportamento de malware no painel administrativo do firewall. Comportamento da rede, comportamento de processo, comportamento de arquivo e informações-chave do arquivo são exibidos nos relatórios. O processo do ataque é visualizado pela análise de Cadeia de Morte nas plataformas de firewall para que os administradores de segurança possam tomar as medidas apropriadas.

Atualização constante do banco de dados de assinatura

O Hillstone Cloud Sandbox gera inteligência de ameaça com base no malware que ele detecta e atualiza as informações de inteligência no banco de dados de assinatura dos Hillstone Next-Generation Firewalls. Isso ajuda os administradores a ajustar as estratégias de segurança para proteger seus recursos de TI de novos ataques mais recentes e avançados.

A Hillstone Cloud Sandbox agora está disponível nos firewalls de próxima geração E-series (NGFW), nos firewalls inteligentes de última geração da T-Series (iNGFW), Hillstone CloudEdge, no sistema de prevenção de intrusões na rede da S-Series (NIPS).

Version: EX-08.01-CloudSandbox-V3.1-0818-PT-02