FIREEYE FX

Prevenção de ameaças de conteúdo

Detecte e elimine malware residente em compartilhamentos de arquivos e armazenamentos de conteúdo

VISÃO GERAL

A plataforma de prevenção de ameaças FireEye® FX protege ativos de dados contra ataques originados em uma ampla gama de tipos de arquivos. Webmail, ferramentas de transferência de arquivos on-line, nuvem e dispositivos portáteis de armazenamento de arquivos podem introduzir um malware capaz então de se espalhar para compartilhamentos de arquivos e repositórios de conteúdo. O FireEye FX analisa compartilhamentos de arquivos em rede e armazenamentos de gerenciamento de conteúdo corporativo para detectar e colocar em quarentena um malware capaz de contornar firewalls de próxima geração, sistemas de prevenção de intrusões, antivírus e gateways.

O problema do malware residente em compartilhamentos de arquivos

Os ataques cibernéticos avançados de hoje usam malware sofisticado e táticas de ameaças persistentes avançadas (APT) para atravessar as defesas e se espalhar lateralmente pelos compartilhamentos de arquivos e repositórios de conteúdo. Isso permite que o malware estabeleça uma presença a longo prazo na rede e infecte múltiplos sistemas, até aqueles que estão off-line. Muitos data centers corporativos continuam especialmente vulneráveis ao malware avançado baseado em conteúdo, porque as defesas tradicionais não são eficientes contra esses ataques, que com frequência entram na rede por meios legítimos. Os criminosos cibernéticos aproveitam essa vulnerabilidade para espalhar malware nos compartilhamentos de arquivos da rede e incorporam código nocivo a vastos repositórios de dados, resultando em uma ameaça persistente mesmo após a correção.

A proteção do conteúdo é essencial para deter o ciclo de vida dos ataques avançados

Sem uma forma de detectar malware no conteúdo, as APTs podem explorar os ativos da rede para extrair informações proprietárias e causar muitos danos. A série FireEye FX analisa compartilhamentos de arquivos e repositórios de conteúdo corporativo usando o mecanismo patenteado FireEye Multi-Vector Virtual Execution™ (MVX), que detecta código nocivo de dia zero incorporado a tipos comuns de arquivos (PDF, MS Office, vCards, ZIP/RAR/TNEF etc.) e conteúdo de multimídia (QuickTime, MP3, Real Player, JPG, PNG etc.). A série FireEye FX executa varreduras recursivas, programadas e sob solicitação em armazenamentos de conteúdo e compartilhamentos de arquivos de rede acessíveis para identificar e colocar em quarentena o malware residente. Isso suspende um estágio fundamental do ciclo de vida dos ataques avançados.

O mecanismo FireEye MVX revela ameaças desconhecidas de dia zero

O FireEye FX usa o mecanismo dedicado FireEye MVX, que inspeciona cada arquivo e confirma a existência de ataques de dia zero ou de código malicioso. O mecanismo FireEye MVX detecta ataques de dia zero, de fluxos múltiplos e outros ataques evasivos com análise dinâmica e sem assinaturas em um ambiente virtual seguro. Ele interrompe as fases de infecção e comprometimento da cadeia de destruição do ataque cibernético identificando malware e exploits nunca antes vistos.

DESTAQUES

- Encontra malware latente que não é detectado pelos mecanismos de antivírus tradicionais.
- Pode ser distribuído em quarentena ativa (modo de proteção) ou somente análise (modo de monitoramento).
- Oferece varreduras recursivas, programadas e sob solicitação de compartilhamentos de arquivos compatíveis com CIFS e NFS.
- Oferece proteção proativa de SharePoint aproveitando o protocolo WebDAV.
- Inclui a análise de uma ampla gama de tipos de arquivos, como PDFs, documentos do Microsoft Office e arquivos de multimídia.
- Integra-se com o pacote antivírus FireEye AV-Suite para simplificar a priorização de respostas a incidentes e as convenções de nomenclatura.
- Compartilha dados sobre ameaças com as plataformas da FireEye por meio da FireEye CM e da FireEye DTI Cloud.

Aproveitando o poder do FireEye MVX Smart Grid

O MVX Smart Grid melhora ainda mais a segurança de rede líder do mundo, incluindo uma arquitetura de implantação flexível e expansível por meio de nuvem híbrida ou privada. O MVX Smart Grid usa uma abordagem inovadora para proteger de maneira mais eficaz campi, filiais e usuários remotos por meio da separação do pioneiro mecanismo MVX da FireEye e do desenvolvimento de hardware e Smart Nodes™ virtuais. Os Smart Nodes analisam o tráfego da Internet para detectar e bloquear ameaças usando várias técnicas, como análises estáticas, análises, IPS, inteligência aplicada e muito mais, enquanto o mecanismo MVX executa a análise dinâmica principal.

Varredura de conteúdo e quarentena proativas para SharePoint

O FireEye FX faz varredura de conteúdo de maneira contínua para alertar e colocar permanentemente em quarentena qualquer malware descoberto em repositórios do SharePoint. A plataforma aproveita o protocolo WebDAV para se integrar com segurança a serviços do SharePoint e proteger fluxos de trabalho corporativos que utilizam repositórios do SharePoint.

Regras com base em YARA permitem personalização

O FireEye FX suporta regras YARA personalizadas para analisar grandes quantidades de arquivos em busca de ameaças específicas à organização.

Priorização de incidentes simplificada

Com o pacote antivírus FireEye AV-Suite, todos os objetos maliciosos podem ser analisados mais minuciosamente para determinar se os fornecedores de antivírus conseguiram detectar o malware detido pelo FireEye EX. Isso permite que as empresas priorizem a resposta a incidentes de forma eficiente e utilizem convenções de nomenclatura comuns para o malware conhecido.

Compartilhamento de inteligência sobre malware

A inteligência resultante sobre ameaças, gerada dinamicamente e em tempo real, pode ajudar todos os produtos da FireEye a proteger a rede local por meio da integração com a plataforma FireEye CM. Essa inteligência pode ser compartilhada globalmente pela nuvem do FireEye Dynamic Threat Intelligence™ (DTI) para notificar todos os assinantes sobre ameaças emergentes.

Nenhum ajuste fino de regras e quase nenhum falso positivo

O FireEye FX é um grupo de plataformas sem clientes, fáceis de gerenciar e que não exigem nenhum ajuste fino. Modos flexíveis de distribuição incluem quarentena ativa e monitoramento apenas para análise. Isso permite que as empresas saibam quanto malware reside em compartilhamentos de arquivos e possam deter ativamente a disseminação lateral do malware.

Smart Nodes de conteúdo oferecem proteção onde você precisa

Com os Smart Nodes de conteúdo da FireEye, gerentes de conteúdo e segurança têm uma solução virtual flexível para proteger conteúdo essencial em toda a empresa. Além disso, combinada com uma plataforma FireEye MVX Smart Grid, a proteção de conteúdo pode ser dimensionada e distribuída com flexibilidade, onde você precisar.

Tabela 1. Smart Node de conteúdo FireEye

	FX 2500V
Sistemas operacionais compatíveis	Microsoft Windows, Mac OS X
Desempenho	70.000 arquivos/dia
Portas de interface de rede	Ether 1, Ether 2
Núcleos de CPU	2
Memória	8 GB
Capacidade das unidades	512 GB
Suporte para hipervisor	VMWare ESXi 6.0 ou posterior

Para obter mais informações sobre a FireEye, visite:
www.FireEye.com

FireEye, Inc.
1440 McCarthy Blvd. Milpitas, CA 95035 tel: 408.321.6300/877.FIREEYE (347.3393)/info@FireEye.com

www.FireEye.com

A FireEye® é líder em segurança como serviço (SaaS) orientada por inteligência. Atuando harmoniosamente como extensão expansível das operações de segurança dos clientes, a FireEye oferece uma plataforma única que mescla tecnologias de segurança inovadoras, inteligência sobre ameaças em nível de país e a consultoria mundialmente reconhecida da Mandiant®. Com essa abordagem, a FireEye elimina a complexidade e o fardo da segurança cibernética para organizações empenhadas em se preparar, prevenir e responder a ataques cibernéticos. A FireEye tem mais de 5.000 clientes em 67 países, incluindo mais de 940 empresas da Forbes Global 2000.

FireEye