FireEye™

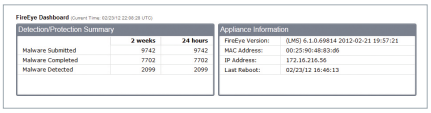
Datasheet

Malware Analysis System

Análise forense de próxima geração para ataques avançados e direcionados

Destaques

- Análises simplificadas e em lote de arquivos, códigos da Web e executáveis suspeitos
- Relatórios detalhados de alterações realizadas por aplicativos e pelo sistema operacional, nos sistemas de arquivo, na memória e nos registros
- Análise em tempo real ou em área restrita (sandbox) para a confirmação de ataques de dia-zero
- Fim dos inconvenientes causados pela distribuição e pela necessidade de ajustes, graças a um ambiente pré-configurado, aliado à automatização da configuração e da eliminação de imagens de testes virtuais
- Geração dinâmica de informações sobre malware para proteção local imediata através da integração com o Central Management System (CMS)
- Captura de pacotes para permitir a análise de execução de código e sessões de URL com fins maliciosos
- Suporte a regras YARA personalizadas (compatível com a versão 1.3)
- Verificação de assinaturas de antivírus incluídas para simplificar a priorização de respostas a incidentes
- Suporta AAA (Authentication, Authorization and Accounting) de terceiros, para acesso a serviços de rede além da autenticação local.



O dashboard do MAS exibe o status de análises concluídas e pendentes do mecanismo VX

O FireEye Malware Analysis System (MAS) oferece aos analistas de ameaças um controle prático sobre ambientes de testes e configurados automaticamente. Eles podem executar e inspecionar com segurança ataques avançados de malware, ataques de dia-zero e ameaças persistentes avançadas e direcionadas em arquivos, anexos de e-mail e objetos da Web.

Os criminosos cibernéticos criam ataques personalizados para penetrar em empresas, contas de usuário ou sistemas específicos. Diante disso, os analistas precisam de ferramentas forenses fáceis de usar e que os ajudem a lidar rapidamente com atividades maliciosas muito direcionadas.

Avaliação de ataques a sistemas operacionais, navegadores e aplicativos

O mecanismo FireEye Virtual Execution (VX) capacita os analistas internos com uma visão de 360 graus de um ataque, cobrindo do ataque inicial aos destinos de callback e às tentativas seguintes de download de binários. Através de um ambiente de análise virtual instrumentado e pré-configurado do Windows, o mecanismo VX executa completamente o código suspeito para permitir uma inspeção profunda de formatos de arquivo comuns, anexos de e-mail e objetos da Web. O FireEye MAS inspeciona arquivos isolados ou lotes de arquivos em busca de malware e rastreia tentativas de conexão de saída em vários protocolos.

Tempo investido na análise, e não na administração

O mecanismo VX oferece hardware de PC virtualizado operando versões completas de sistemas operacionais da Microsoft, além de navegadores, plug-ins e outros aplicativos de terceiros. O appliance MAS libera os administradores das demoradas tarefas de configuração, criação de linha de base e restauração dos ambientes de máquina virtual usados em análises manuais de malware.

"Um dos grandes atrativos da solução da FireEye é que ela realiza análises em um ambiente de execução virtual para determinar se um código sinalizado realmente é uma ameaça. Essa análise gera informações detalhadas que nos permitem identificar a melhor opção para resolver um problema. Ela nos permite saber exatamente como reagir."

— Diretor de segurança cibernética do setor de energia

Modos de análise em área restrita e "Honeypot"

No modo de área restrita (sandbox), os pesquisadores podem testemunhar o caminho de execução de amostras específicas de malware, além de gerar um perfil dinâmico e anonimizado do ataque, que pode ser distribuído pelo CMS para outros appliances Web, Email e File Malware Protection System (MPS) da FireEye. Os perfis de ataque de malware incluem identificadores de código de malware, URLs de ataque e outras fontes de infecções e ataques. Além disso, as características dos protocolos de comunicação do malware são compartilhadas para que seja oferecido um bloqueio dinâmico das tentativas de evasão de dados.

Além das análises em área restrita, o FireEye oferece um modo "pote de mel" (honeypot) ao vivo na rede para análise do ciclo de vida completo do malware. O malware avançado de hoje contorna a segurança tradicional desdobrando-se em vários estágios. O primeiro estágio do ataque, vulnerabilidade apenas estabelece um porto seguro para os criminosos.

A FireEye integra inspeções de entrada e saída em diversos protocolos para uma análise abrangente de ameaças contra sistemas operacionais, Web, e-mail e aplicativos que atacam por meio de vários vetores.

Regras com base em YARA para personalização

O MAS permite a importação de regras YARA personalizadas para especificar regras em nível de byte e analisar rapidamente objetos suspeitos em busca de ameaças específicas à organização. As regras personalizadas são usadas como parte da análise do mecanismo VX para identificar prováveis objetos maliciosos, bem como objetos classificados anteriormente como maliciosos.

Rede global de proteção contra malware

O Malware Analysis System pode compartilhar automaticamente dados de perícia de malware com outros appliances MPS através do FireEye CMS para bloquear as tentativas de evasão de dados de saída e os ataques conhecidos de entrada. Os dados de ameaças do MAS também podem ser compartilhados pelo FireEye Malware Protection Cloud (MPC) para proteção contra ataques emergentes.

Com mecanismos pré-configurados de execução virtual que acabam com a necessidade de ajustes heurísticos, o FireEye MAS poupa ao administrador tempo e aborrecimento com a configuração. Essa solução econômica e fácil de gerenciar ajuda os pesquisadores de ameaças a analisar ataques avançados e direcionados sem gerar sobrecarga do gerenciamento da rede e da segurança.

Especificações técnicas

	MAS 4310	MAS 7300	MAS 8300
Formato físico	1U para montagem em Rack	1U para montagem em Rack	2U para montagem em Rack
Peso	13,6 kg	13,6 kg	22,7 kg
Dimensões (LxPxA)	43,7 x 65,0 x 4,3 cm	43,7 x 65,0 x 4,3 cm	43,7 x 70,9 x 8,9 cm
Gabinete	Para Rack de 19"	Para Rack de 19"	Para Rack de 19"
Portas de gerenciamento	2 portas 10/100/1000 BASE-T	2 portas 10/100/1000 BASE-T	2 portas 10/100/1000 BASE-T
Portas de monitoramento	N/D	N/D	2 portas 10/100/1000 BASE-T
Desempenho	Até 25.000 objetos por dia	Até 50.000 objetos por dia	Até 100.000 objetos por dia
Tensão de entrada CA	100 ~ 240 VCA com comutação automática	100 ~ 240 VCA com comutação automática	100 ~ 240 VCA com comutação automática
Corrente de entrada CA	8,5 - 6,0 A	8,5 - 6,0 A	9,5 - 7,2 A
Fonte de alimentação/RAID	Dupla de 700 W / 2 discos rígidos SAS em RAID1 por hardware	Dupla de 700 W / 2 discos rígidos SAS em RAID1 por hardware	Dupla de 1.400 W / 2 discos rígidos SAS em RAID1 por hardware
Frequência	50 - 60 Hz	50 - 60 Hz	50 - 60 Hz
Temperatura de funcionamento	10° C a 35° C.	10° C a 35° C.	10° C a 35° C.

Observação: Todos os valores de desempenho variam dependendo da configuração do sistema e do perfil de tráfego sendo processado.