FIREEYE™

FICHA TÉCNICA

Análise de malware

Analisa ataques com visibilidade de 360 graus

DESTAQUES

- Executa análises forenses profundas em todo o ciclo de vida do ataque usando o mecanismo FireEye MVX
- Análises simplificadas e em lote de códigos da Web, executáveis e arquivos suspeitos
- Relatórios detalhados de alterações em nível de sistema realizadas por aplicativos e pelo sistema operacional, em sistemas de arquivos, memória e registros
- Análise ao vivo ou em sandbox para a confirmação de ataques de dia-zero
- Geração dinâmica de inteligência sobre ameaças para proteção local imediata por meio da integração com o FireEye Central Management
- Captura de pacotes para permitir a análise de execução de código e sessões de URL com fins maliciosos
- Inclui o pacote antivírus FireEye AV-Suite para simplificar a priorização de respostas a incidentes
- Compatível com ambientes Windows e MacOS X

Figura 1. Appliance FireEye Malware Analysis AX 5550.

Visão geral

O FireEye Malware Analysis é uma solução de análise forense que oferece aos analistas de segurança um controle prático sobre ambientes de testes poderosos e configurados automaticamente, a fim de executar e inspecionar com segurança ataques avançados de malware, ataques de dia zero e ameaças persistentes avançadas (Advanced Persistent Threat, APT) incorporadas em páginas da Web, anexos de e-mail e arquivos.

Conforme os criminosos cibernéticos criam ataques personalizados para invadir empresas, contas de usuário ou sistemas específicos, os analistas precisam de ferramentas forenses fáceis de usar e que os ajudem a lidar rapidamente com atividades nocivas direcionadas.

Avaliação de ataques a sistemas operacionais, navegadores e aplicativos

O Malware Analysis usa o mecanismo FireEye Multi-Vector Virtual Execution™ (MVX) para dar aos analistas internos uma visão completa, de 360 graus, de um ataque, desde o ataque inicial até os destinos de comunicação de retorno e as tentativas subsequentes de download de binários.

Por meio de um ambiente de análise virtual do Microsoft Windows e do Apple MacOS X instrumentado e pré-configurado, o mecanismo MVX executa o código suspeito em sua totalidade para permitir uma inspeção profunda de objetos comuns da Web, anexos de e-mail e arquivos. O Malware Analysis usa o mecanismo MVX para inspecionar 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 Malware Analysis 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. Com personalização integrada e controle granular sobre a detonação de cargas maliciosas, o Malware Analysis permite que os analistas forenses obtenham uma compreensão abrangente do ataque, adequada para as necessidades da empresa.

Opção de análise nos modos ao vivo ou sandbox

O Malware Analysis fornece aos usuários dois modos de análise: ao vivo e sandbox. Os analistas de malware usam o modo ao vivo, com acesso à rede, para fazer a análise do ciclo de vida completo do malware, permitindo conectividade externa. Isso dá ao Malware Analysis a capacidade de rastrear ataques avançados em múltiplos estágios e diferentes vetores. No modo sandbox, o caminho de execução das amostras de malware é completamente isolado e visível no ambiente virtual.

Em ambos os modos, os usuários podem gerar um perfil dinâmico e anônimo do ataque, que pode ser compartilhado pelo FireEye Central Management com outras soluções da FireEye. Os perfis de ataque de malware gerados pelo Malware Analysis incluem identificadores de código de malware, URLs de ataque e outras fontes de infecções e ataques. Além disso, as características do protocolo de comunicação do malware são compartilhadas para proporcionar o bloqueio dinâmico de tentativas de vazamento de dados em toda a distribuição da FireEye na organização, pelo FireEye Dynamic Threat Intelligence™ (DTI).

Regras com base em YARA permitem personalização

O Malware Analysis 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.

Rede global de proteção contra malware

O Malware Analysis pode compartilhar automaticamente dados forenses de malware com outras soluções FireEye por meio do Central Management para bloquear as tentativas de evasão de dados de saída e os ataques conhecidos de entrada. Os dados de ameaças do Malware Analysis podem ser compartilhados pela nuvem FireEye DTI para proteção contra ataques emergentes.

Com mecanismos FireEye MVX pré-configurados que eliminam a necessidade de ajustes heurísticos, o Malware Analysis poupa ao administrador tempo e aborrecimento com a configuração. Essa solução também ajuda os pesquisadores de ameaças a analisar ataques avançados e direcionados sem gerar sobrecarga do gerenciamento da rede e da segurança.

Tabela 1. Especificações técnicas.

	AX 5550
Desempenho *	Até 8.200 análises por dia
Sistemas operacionais compatíveis	Microsoft Windows/Apple Mac OSX
Portas de interface de rede	2 portas 10/100/1000 BASE-T
Porta IPMI (painel traseiro)	Incluídas
Teclado numérico	Incluídas
Portas DB15 VGA (painel traseiro)	Incluídas
Portas USB (painel traseiro)	4 portas USB tipo A
Porta serial (painel traseiro)	115.200 bps, sem paridade, 8 bits, 1 stop bit
Capacidade das unidades	2 unidades de disco rígido de 4 TB, RAID 1, 3,5", FRU
Gabinete	1 RU, para rack de 19"
Dimensões do chassi (L x P x A)	437 mm x 650 mm x 43,2 mm
Fonte de alimentação CC	Não disponível
Fonte de alimentação CA	Redundante (1+1) 750 watts, 100–240 VCA, 8–4,5A, 50–60 Hz, entrada IEC60320-C14, FRU
Consumo de energia máximo	225 W
Dissipação térmica máxima	768 BTU/h

Tabela 1. Especificações técnicas.

	AX 5550
Tempo médio entre falhas (MTBF)	54.200 h
Peso líquido/total (kg)	12,2 kg/17,2 kg
Certificações de segurança	IEC 60950, EN 60950, CSA 60950-00, marcação CE
Certificações EMC/EMI	FCC (parte 15, classe A), CE (classe A), CNS, AS/NZS, VCCI (classe A)
Conformidade regulatória	RoHS, REACH, WEEE
Temperatura de funcionamento	0–40 °C
Umidade relativa de funcionamento	10–95% a 40 °C, sem condensação
Altitude de funcionamento	3.000 m

Observação: os valores de desempenho são baseados nos tempos padrão de análise com o Malware Analysis, mas podem variar de acordo com a configuração do sistema e os perfis de tráfego sendo processados.

Para saber mais sobre a FireEye, visite: **www.FireEye.com**

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

Sobre a FireEye, Inc.

A FireEye é a empresa líder em segurança 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 de ameaças em nível governamental 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.