FIREEYE™

FICHE PRODUIT

Malware Analysis

Analysez les attaques à l'aide d'une visibilité à 360 °

EN BREF

- Réalise une analyse forensique approfondie sur l'ensemble du cycle de vie de l'attaque à l'aide du moteur FireEye MVX
- Rationalise et organise par lots l'analyse des fichiers, des exécutables et du code web suspects
- Propose des rapports détaillés sur les modifications apportées aux systèmes de fichiers, à la mémoire et aux registres au niveau du système d'exploitation et des applications de chaque système
- Fournit une analyse en mode sandbox ou en mode réel pour confirmer les exploits zero-day
- Génère une Threat Intelligence de manière dynamique pour assurer la protection immédiate de l'environnement local via l'intégration avec la plateforme FireEye Central Management
- Capture les paquets pour analyser l'exécution de code et les sessions se connectant à des URL malveillantes
- Comprend FireEye AV-Suite pour optimiser l'établissement de priorités lors de la réponse à incident
- Prise en charge des environnements Windows et Mac OS X

Figure 1. Appliance FireEye Malware Analysis AX 5550

Présentation

FireEye Malware Analysis est une solution d'analyse forensique qui procure aux experts de la sécurité un contrôle en interne sur des environnements de test puissants auto-configurés. Ceux-ci leur permettent d'exécuter et d'examiner en toute sécurité des malwares avancés, des menaces zero-day et des menaces APT incorporés dans des fichiers, des pièces jointes et des pages web.

À l'heure où les cybercriminels personnalisent leurs attaques pour s'infiltrer dans des environnements d'entreprise, des comptes utilisateurs ou des systèmes spécifiques, les analystes ont besoin d'outils forensiques qui les aident à traiter ces menaces ciblées.

Évaluation des attaques exploitant les systèmes d'exploitation, les navigateurs et les applications

Malware Analysis exploite le moteur FireEye Multi-Vector Virtual Execution™ (MVX) pour fournir aux analystes internes une vue à 360 ° de l'attaque — de l'exploit initial jusqu'aux destinations des rappels et aux tentatives de téléchargement binaire qui s'ensuivent.

Le moteur MVX exécute en intégralité le code suspect dans un environnement d'analyse virtuel Microsoft Windows et Apple Mac OS X instrumenté et préconfiguré, permettant ainsi une inspection approfondie des fichiers, des pièces jointes et des objets web courants. Grâce à lui, Malware Analysis est en mesure d'inspecter des fichiers isolés ou par groupes pour y détecter d'éventuels malwares et tentatives de connexions sortantes sur plusieurs protocoles.

Moins d'administration, plus d'analyses

Malware Analysis libère les administrateurs des tâches fastidieuses d'installation, de configuration des valeurs de référence et de restauration des environnements de machines virtuelles utilisés lors de l'analyse manuelle. Elle propose aux analystes forensiques une fonction de personnalisation intégrée et un contrôle granulaire sur les déclenchements de payloads. Ils parviennent ainsi à cerner toutes les facettes de l'attaque dans un contexte spécifique à l'entreprise.

Analyse en environnement réel ou en sandbox

Malware Analysis propose deux modes d'analyse : en environnement réel ou dans le confinement d'une sandbox. Les spécialistes des malwares utilisent le mode réseau actif en temps réel pour analyser le cycle de vie complet du malware tout en préservant une connectivité externe. Ce mode permet à la solution de repérer des attaques avancées à divers stades d'exécution et sur différents vecteurs. En mode sandbox, le chemin d'exécution des échantillons de malware est parfaitement isolé et visible au sein d'un environnement virtuel.

Ces deux modes permettent à l'utilisateur de générer un profil dynamique et anonymisé de l'attaque, qu'il peut ensuite partager avec d'autres produits FireEye via la plateforme FireEye Central Management. Les profils générés par Malware Analysis incluent les identifiants et le code du malware, les URL d'exploit et d'autres sources d'infections et d'attaques. Les caractéristiques du protocole de communication du malware sont également mises en commun, permettant ainsi à FireEye Dynamic Threat Intelligence™ (DTI) de bloquer de manière dynamique les tentatives d'exfiltration de données sur l'ensemble du déploiement FireEye dans l'entreprise.

Personnalisation à l'aide de règles YARA

Malware Analysis permet l'importation de règles YARA personnalisées afin d'établir des règles au niveau de l'octet et d'analyser rapidement les objets suspects au regard du profil de risque de l'entreprise.

Réseau mondial de protection anti-malware

Malware Analysis partage automatiquement les données forensiques sur les malwares avec d'autres solutions FireEye via FireEye Central Management, empêche les tentatives d'exfiltration de données en sortie et bloque les attaques connues en entrée. La Threat Intelligence de Malware Analysis peut aussi être partagée au travers du cloud FireEye DTI afin d'assurer une protection contre les nouvelles attaques émergentes.

Le moteur FireEye MVX préconfiguré de Malware Analysis rend inutile tout paramétrage de l'analyse heuristique, ce qui permet aux administrateurs de passer moins de temps sur le déploiement et la configuration. En outre, la solution aide les traqueurs de menaces à analyser les attaques ciblées avancées sans augmenter la charge sur le réseau ni les frais de gestion de la sécurité.

Tableau 1. Spécifications techniques

	AX 5500
Performances*	Jusqu'à 8 200 analyses par jour
Systèmes d'exploitation pris en charge	Microsoft Windows / Apple Mac OS X
Ports de l'interface réseau	2 ports 10/100/1000 BASE-T
Port IPMI (panneau arrière)	Inclus
Pavé numérique	Inclus
Port VGA DB15 (panneau arrière)	Inclus
Ports USB (panneau arrière)	4 ports USB de type A
Port série (panneau arrière)	115 200 bit/s, pas de parité, 8 bits, 1 bit d'arrêt
Capacité des disques	2 disques durs de 4 To, RAID 10, 3,5 pouces, remplaçables
Châssis	Montage en baie 1U, s'intègre en baie 19 pouces
Dimensions du châssis (L x P x H)	43,7 x 65 x 4,32 cm
Alimentation en courant continu	Non disponible
Alimentation en courant alternatif	Redondante (1+1) 750 W, 100– 240 VCA, 8–4,5 A, embase secteur IEC 60320-C14, 50 – 60 Hz, remplaçable
Consommation électrique maximale	225 W

Tableau 1. Spécifications techniques

	AX 5500
Dissipation thermique maximale	768 BTU/h
Temps moyen de bon fonctionnement	54 200 h
Poids de l'appliance seule/ avec emballage	12,2 kg / 17,2 kg
Certifications de sécurité	IEC 60950, EN 60950, CSA 60950-00, Marquage CE
Certifications EMC/EMI	FCC (article 15, classe A), CE (classe A), CNS, AS/NZS, VCCI (classe A)
Conformité réglementaire	RoHS, REACH, DEEE
Température de fonctionnement	0-40 °C
Plage d'humidité relative tolérée	10 ~ 95 % à 40 °C, sans condensation
Altitude maximale de fonctionnement	3 000 m

Remarque : les performances mentionnées dans le tableau sont fondées sur les temps d'analyse observés en utilisant Malware Analysis – celles-ci peuvent varier en fonction de la configuration système et du profil du trafic traité.

Pour en savoir plus, rendez-vous sur **www.fireeye.fr**

FireEye, France | Nextdoor Cœur Défense
110 Esplanade du Général de Gaulle
92931 Paris La Défense Cedex 92974
+33 1 70 61 27 26
france@FireEye.com | www.FireEye.fr
FireEye, Inc. | 601 McCarthy Blvd.
Milpitas, CA 95035 | +1 408 321 6300
info@FireEye.com

À propos de FireEye, Inc.
FireEye est spécialisé dans la cybersécurité axée sur la Cyber Threat Intelligence (CTI). Prolongement naturel et évolutif des opérations de sécurité des clients, la plateforme unique de FireEye combine des technologies de sécurité innovantes, des services de CTI d'envergure internationale et les services réputés de Mandiant® Consulting. FireEye simplifie ainsi la cybersécurité et son administration, devenant un allié précieux des entreprises confrontées au casse-tête que représentent la prévention et la neutralisation des cyberattaques.

FIREEYE™