FireEye

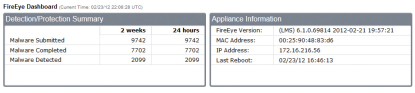
Specyfikacja urządzenia

Malware Analysis System

Nowa generacja szczegółowej analizy zaawansowanych ataków

Główne cechy:

- Optymalizacja i grupowanie analiz podejrzanych plików, kodu stron Web i jego wykonania
- Dogłębne raporty dotyczące zmian w systemach operacyjnych i aplikacjach mających wpływ na system plików, pamięć oraz rejestry
- Tryby sandbox lub live służące potwierdzeniu exploitów typu zero-day
- Nie sprawia problemów w instalacji, nie trzeba dostosowywać go do aktualnych ustawień systemu - posiada automatyczną konfigurację
- Dynamiczne generowanie informacji o malware zapewnia natychmiastową ochronę lokalnej sieci poprzez integrację z FireEye Central Management System™ (CMS)
- Przechwytywane pakiety umożliwiają analizę złośliwych sesji URL oraz realizację zawartego w nich kodu
- Wsparcie niestandardowych reguł YARA (kompatybilne z wersją 1.3)
- Zawarty AV Suite usprawnia ustalanie priorytetów przy reagowaniu na incydenty
- Wsparcie zdalnego dostępu do sieci, poprzez zewnętrzne usługi AAA (autentication, authorization i accounting) oraz autentykacji lokalnej



Panel kontrolny MAS ukazuje status trwających i zakończonych analiz wykonywanych przez silnik VX

FireEye Malware Analysis System (MAS) dostarcza analitykom bezpośrednią kontrolę nad wydajnym samo konfigurowalnym środowiskiem testowym, które pozwala na bezpieczne uruchamianie i sprawdzanie zaawansowanego malware, ataków zero-day oraz ukierunkowanych ataków APT zakodowanych w plikach, załącznikach email oraz w obiektach Web.

Cyberprzestępcy dostosowują ataki do profilu przedsiębiorstwa, specyfiki kont użytkowników lub systemu, więc analitycy potrzebują łatwego w użyciu narzędzia, które pomoże im szybko lokalizować bardzo ukierunkowaną złośliwą działalność.

Ocena ataków na system operacyjny, przeglądarki i aplikacje

FireEye Virtual Execution (VX) engine™ dostarcza analitykom narzędzie zapewniające pełny obraz ataku, od początkowego exploitu do destynacji wywołania zwrotnego oraz umożliwia śledzenie prób pobierania danych. Silnik VX wykonuje pełną ścieżkę podejrzanego kodu przez zdefiniowane wirtualne środowisko Windows, aby umożliwić dogłębną inspekcję popularnych formatów plików, załączników email i obiektów Web. FireEye MAS wykrywa pliki lub grupy plików malware i śledzi generowane przez nie próby połączeń wychodzących przez wiele protokołów.

Poświęcaj czas na analizę, nie administrowanie

Silnik VX funkcjonuje jako wirtualny komputer PC używający pełnej gamy systemów operacyjnych Microsoftu, przeglądarek, plug-inów oraz aplikacji. Urządzenie MAS uwalnia administratorów od czasochłonnego konfigurowania, resetowania i przywracania wirtualnego środowiska używanego przy manualnej analizie malware.

Wybierz tryb *sandbox* lub *honeypot*

W trybie ***sandbox*** możliwe jest obserwowanie uruchomienia i wykonywania fragmentu ścieżki malware, a także generowanie dynamicznych profili ataku, które mogą być udostępniane przez CMS innym urządzeniom FireEye (Web, Email, File MPS). Profil ataku malware zawiera identyfikator kodu, URL exploit i inne źródła infekcji. Poza tym, udostępniana jest charakterystyka protokołu wykorzystywanego przez malware do komunikacji, w celu zapewnienia dynamicznego blokowania prób kradzieży danych.

„Jedną z wielkich zalet rozwiązania FireEye jest to, że analizy odbywają się w wirtualnym środowisku w celu sprawdzenia, czy oznaczony fragment kodu stanowi faktyczne zagrożenie. Szczegółowe informacje, które są generowane pozwalają na określenie najlepszego sposobu rozwiązania problemu. Dzięki temu dokładnie wiemy jak reagować na incydenty"

Director of Cyber Security, Energy Sector

Tryb ***honeypot*** umożliwia analizę pełnego cyklu życia malware w czasie rzeczywistym. Dzisiejszy, zaawansowany malware omija tradycyjne zabezpieczenia poprzez wieloetapowy rozwój. Pierwsza faza – exploit służy jedynie jako punkt zaczepienia dla cyberprzestępców.

FireEye łączy kontrolę ruchu przychodzącego i wychodzącego przez wiele protokołów w celu stworzenia obszernej analizy zagrożeń systemu operacyjnego, środowiska Web, email i aplikacji oraz ataków wielowektorowych.

Reguły YARA pozwalają na indywidualizację

MAS umożliwia import niestandardowych reguł YARA, które pozwalają sprecyzować reguły *byte-level* i szybko zbadać podejrzane obiekty na istnienie zagrożeń charakterystycznych dla organizacji. Niestandardowe reguły są używane przy analizie przez silnik VX w celu identyfikacji potencjalnie złośliwych obiektów, a także obiektów wcześniej uznanych za złośliwe.

Globalna sieć ochrony przed malware

Malware Analysis System może automatycznie udostępniać informacje o malware innym urządzeniom FireEye MPS poprzez FireEye CMS, żeby w pełni zablokować próby kradzieży danych i powstrzymać wcześniej rozpoznane ataki. Informacje te mogą być również współdzielone przez FireEye Malware Protection Cloud™ (MPC) żeby ostrzegać innych subskrybentów przed powstającymi atakami.

FireEye MAS oszczędza czas potrzebny na konfigurację. Jest to rozwiązanie łatwe w zarządzaniu, efektywne kosztowo i pomaga w analizie zaawansowanych, ukierunkowanych ataków, bez obciążania osób zarządzających siecią i jej bezpieczeństwem.

Specyfikacja techniczna

	MAS 4310	MAS 7300	MAS 8300
Obudowa	1U Rack	1U Rack	2U Rack
Waga	13,6 kg	13,6 kg	22,7 kg
Wymiary (szer. x głęb. x wys. cm)	43,7 x 65,0 x 4,3	43,7 x 65,0 x 4,3	43,7 x 70,9 x 8,9
Mocowanie	19-calowy Rack	19-calowy Rack	19-calowy Rack
Porty do zarządzania	(2) 10/100/1000 BASE-T Ports	(2) 10/100/1000 BASE-T Ports	(2) 10/100/1000 BASE-T Ports
Porty do monitorowania	-	-	(2) 10/100/1000 BASE-T Ports
Wydajność	do 25 000 obiektów dziennie	do 50 000 obiektów dziennie	do 100 000 obiektów dziennie
AC input voltage	Auto-switching 100~240 V AC Full Range	Auto-switching 100~240 V AC Full Range	Auto-switching 100~240 V AC Full Range
AC input current	8,5-6,0 A	8,5-6,0 A	9,5-7,2 A
Zasilanie/RAID	Dual 700W / 2 SAS HDD in HW RAID 1	Dual 700W / 2 SAS HDD in HW RAID 1	Dual 1400W / 2 SAS HDD in HW RAID 1
Częstotliwość	50-60 Hz	50-60 Hz	50-60 Hz
Temp. pracy	10°C - 35°C	10°C - 35°C	10°C - 35°C

UWAGA: niektóre parametry techniczne mogą różnić się w zależności od rodzaju ruchu i konfiguracji systemu